(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2002164899 A

(43) Date of publication of application: 07.06.02

(51) Int. Cl H04L 12/28
H04L 12/24
H04L 12/26
H04L 29/14

(21) Application number: 2000358073

(22) Date of filing: 24.11.00

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

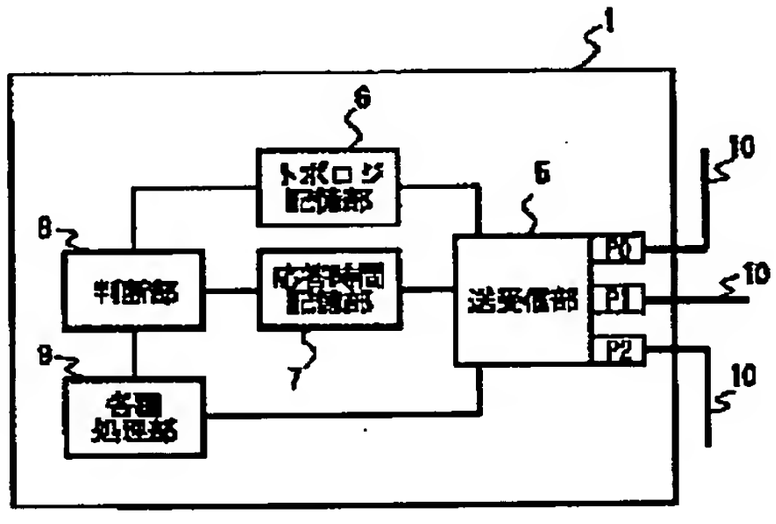
(72) Inventor: SASAKI TAKETO
SHINOHARA TOSHIAKI

(54) NETWORK MONITORING METHOD AND ITS EQUIPMENT

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a network monitoring method and its equipment for finding and taking countermeasure against disguise of a device.

SOLUTION: The network monitoring equipment of the invention is provided with a topology memory part 6 which stores topological information of the network, a response time memory part 7 which stores obtained response time after execution of a response inspection command, and a decision part 8 which decides the consistency between the topological information stored in the topology memory part 6 and the response time stored in the response time memory part 7, and it finds and takes a countermeasure against disguise of a device in a network like IEEE1394 by which such topology can be obtained.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号
特開2002－164899
(P2002－164899A)
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
H04L	12/28		H04L	11/00	310A	5K030
	12/24			11/08		5K033
	12/26			13/00	313	5K035
	29/14					

審査請求　未請求　請求項の数55　ＯＬ　（全 28 頁）

(21)出願番号　特願2000－358073(P2000－358073)

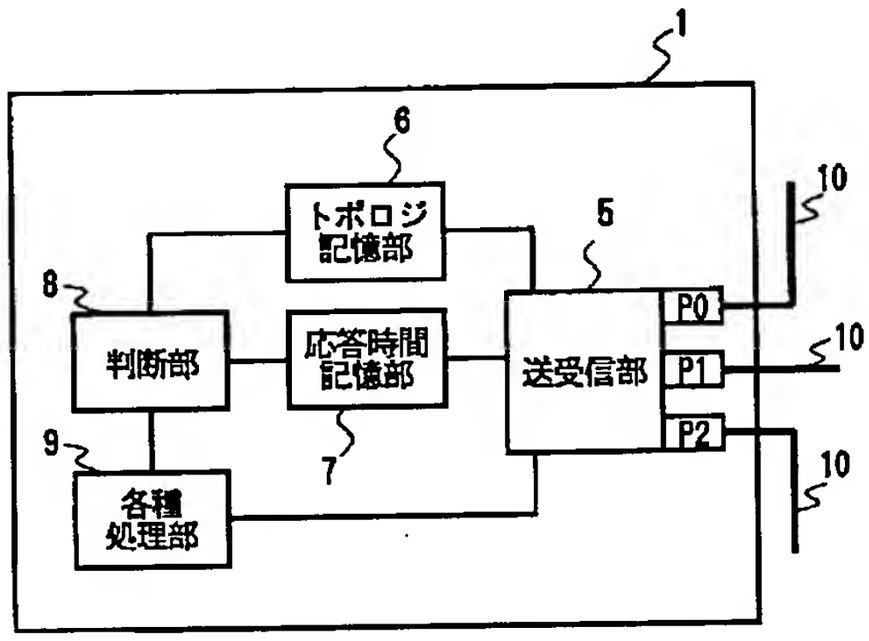
(22)出願日　平成12年11月24日(2000.11.24)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　佐々木　雄飛
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内
(72)発明者　篠原　利章
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内
(74)代理人　100072604
弁理士　有我　軍一郎

最終頁に続く

(54)【発明の名称】　ネットワーク監視方法および装置

(57)【要約】
【課題】　機器のなりすましを発見並びに対策するネットワーク監視方法および装置を提供すること。
【解決手段】　本発明のネットワーク監視装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部６と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部７と、トポロジ記憶部６に記憶されたトポロジ情報と、応答時間記憶部７に記憶された応答時間との整合性を判断する判断部８とを備え、ＩＥＥＥ１３９４のようなトポロジが得られるネットワークにおいて機器のなりすましを発見し対策を行う。



【特許請求の範囲】
【請求項１】　ネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することを特徴とするネットワーク監視方法。
【請求項２】　ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、
前記記憶されたトポロジ情報と、前記記憶された応答時間との整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項３】　ネットワークのトポロジ情報を記憶し、パケットを受信したポートを識別し、
受信パケットのソースＩＤを識別し、
前記記憶されたトポロジ情報と、前記識別されたポートと前記識別されたソースＩＤの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項４】　ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、
前記ネットワークのバスの状態が、ｇｒａｎｔ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定し、
受信パケットのソースＩＤを識別し、
前記記憶されたトポロジ情報と、前記記憶された応答時間と、前記測定された時間と前記識別されたソースＩＤの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項５】　ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、
前記ネットワークのバスの状態が、ｄａｔａ　ｅｎｄ状態からｒｅｑｕｅｓｔ状態に変化するまでの時間を測定し、
受信パケットのソースＩＤを識別し、
前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースＩＤとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項６】　ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、
バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定し、
受信パケットのソースＩＤを識別し、
前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースＩＤとの組み合わせとの整合性を判断することで、がネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項７】　ネットワークのトポロジ情報を記憶し、連続してパケットを受信した場合に、この受信した各パケットのソースＩＤとその受信順番を識別し、
前記記憶されたトポロジ情報と、前記受信したパケットのソースＩＤと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項８】　ネットワークのトポロジ情報を記憶し、ＡＣＫとデータパケットを連続して受信した場合に、この受信した各パケットのソースＩＤとその受信順番を識別し、
前記記憶されたトポロジ情報と、前記受信したパケットのソースＩＤと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項９】　ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、
バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定し、
受信ＡＣＫパケットのソースノードを識別し、
前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたＡＣＫパケットのソースノードとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。
【請求項１０】　前記識別されたソースＩＤがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、
前記ソースＩＤと前記ルーティングテーブルとが矛盾する場合を発見することを特徴とする請求項３乃至請求項８の何れかに記載のネットワーク監視方法。
【請求項１１】　受信パケットのソースＩＤを識別し、
この識別されたソースＩＤがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、
前記ソースＩＤと前記ルーティングテーブルとが矛盾する場合を発見することを特徴とする請求項９に記載のネットワーク監視方法。
【請求項１２】　バスリセットをトリガとして、判断に使用する情報の収集を開始することを特徴とする請求項２乃至請求項１１の何れかに記載のネットワーク監視方法。
【請求項１３】　矛盾を発見した場合に、前記パケットを破棄することを特徴とする請求項２乃至請求項１２の何れかに記載のネットワーク監視方法。
【請求項１４】　矛盾を発見した場合に、前記パケット

を破壊することを特徴とする請求項２乃至請求項１２の何れかに記載のネットワーク監視方法。
【請求項１５】　矛盾を発見した場合に、バスリセットを発生させることを特徴とする請求項２乃至請求項１２の何れかに記載のネットワーク監視方法。
【請求項１６】　矛盾を発見した場合に、警告を発生することを特徴とする請求項２乃至請求項１２の何れかに記載のネットワーク監視方法。
【請求項１７】　矛盾を発見した場合に、ポートを切り離すことを特徴とする請求項２乃至請求項１２の何れかに記載のネットワーク監視方法。
【請求項１８】　ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することを特徴とするネットワーク監視装置。
【請求項１９】　ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間との整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２０】　少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、
ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
パケットを受信したポートを識別するポート識別部と、
前記受信パケットのソースＩＤを識別するソース識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記ポート識別部に識別されたポートと前記ソース識別部に識別されたソースＩＤの組み合わせとの整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２１】　複数のポータルを持つブリッジを含むネットワーク監視装置において、前記ブリッジが、
ルーティング情報を記憶するルーティング記憶部と、
パケットを受信したポータルを識別するポータル識別部と、
前記受信パケットのソースＩＤを識別するソース識別部と、
前記ルーティング記憶部に記憶されたルーティング情報と、前記ポータル識別部で識別されたポータルと前記ソース識別部で識別されたソースＩＤの組み合わせとの整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２２】　少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、
ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、
バスの状態がｇｒａｎｔ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定する時間測定部と、
受信パケットのソースＩＤを識別するソース識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別された前記ソースＩＤの組み合わせとの整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２３】　少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、
ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、
バスの状態がｄａｔａ　ｅｎｄ状態からｒｅｑｕｅｓｔ状態に変化するまでの時間を測定する時間測定部と、
受信パケットのソースＩＤを識別するソース識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソースＩＤとの組み合わせの情報の整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２４】　少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、
ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、
バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定する時間測定部と、
受信パケットのソースＩＤを識別するソース識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソー

スＩＤの組み合わせとの整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２５】　少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、
ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
パケットの連続を受信した場合に、それぞれのパケットのソースＩＤとその受信順番を識別するソース順番識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記ソース順番識別部で識別されたソースＩＤとその受信順番との整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２６】　少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、
ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
ＡＣＫとデータパケットの連続を受信した場合に、それぞれのパケットのソースＩＤとその受信順番を識別するＡＣＫソース順番識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記ＡＣＫソース識別部で識別されたソースＩＤとその受信順番との整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２７】　少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、
ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、
バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定する時間測定部と、
受信ＡＣＫパケットのソースノードを識別するソース識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたＡＣＫパケットの前記ソースノードの組み合わせとの整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。
【請求項２８】　ブリッジのルーティングテーブルを確認するルーティングテーブル確認部と、
前記ソース識別部で識別されたソースＩＤと、前記ルーティングテーブル確認部で確認されたブリッジの前記ルーティングテーブルとの整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とする請求項２０乃至請求項２６の何れかに記載のネットワーク監視装置。
【請求項２９】　パケットのソースＩＤを識別するソース識別部と、
ブリッジのルーティングテーブルを確認するルーティングテーブル確認部と、
前記ソース識別部で識別されたソースＩＤと、前記ルーティングテーブル確認部で確認されたブリッジの前記ルーティングテーブルとの整合性を判断する判断部とを具備し、
ネットワークトポロジ上矛盾する場合を発見することを特徴とする請求項２７に記載のネットワーク監視装置。
【請求項３０】　バスリセットをトリガとして、前記判断部で使用する情報の収集を開始することを特徴とする請求項１９乃至請求項２９の何れかに記載のネットワーク監視装置。
【請求項３１】　矛盾を発見した場合に、前記パケットを破棄するパケット破棄処理部を具備することを特徴とする請求項１９乃至請求項３０の何れかに記載のネットワーク監視装置。
【請求項３２】　矛盾を発見した場合に、前記パケットを破壊するパケット破壊処理部を具備することを特徴とする請求項１９乃至請求項３０の何れかに記載のネットワーク監視装置。
【請求項３３】　矛盾を発見した場合に、バスリセットを発生させるバスリセット発生処理部を具備することを特徴とする請求項１９乃至請求項３０の何れかに記載のネットワーク監視装置。
【請求項３４】　矛盾を発見した場合に、警告を発生する警告発生処理部を具備することを特徴とする請求項１９乃至請求項３０の何れかに記載のネットワーク監視装置。
【請求項３５】　矛盾を発見した場合に、ポートを切り離すポート接続制御処理部を具備することを特徴とする請求項１９乃至請求項３０の何れかに記載のネットワーク監視装置。
【請求項３６】　ネットワークのトポロジ情報を記憶し、
パケットのデスティネイションＩＤを識別し、
前記トポロジ情報と前記デスティネイションＩＤの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピートするポートと、ダミー情報をリピートするポートとを決定することを特徴とするリピート方法。

【請求項３７】　バスリセットをトリガとして、前記情報の収集を開始することを特徴とする請求項３６に記載のリピート方法。
【請求項３８】　ネットワークのトポロジ情報を記憶するトポロジ記憶部と、
パケットのデスティネイションＩＤを識別するデスティネイション識別部と、
前記トポロジ記憶部に記憶されたトポロジ情報と前記デスティネイション識別部で識別されたデスティネイションＩＤの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピートするポートと、ダミー情報をリピートするポートとを決定するポート制御部とを具備することを特徴とするリピータ装置。
【請求項３９】　バスリセットをトリガとして、前記情報の収集を開始することを特徴とする請求項３８に記載のリピータ装置。
【請求項４０】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態をユーザに通知することを特徴とするネットワーク保護方法。
【請求項４１】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴とするネットワーク保護方法。
【請求項４２】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を記録することを特徴とするネットワーク保護方法。
【請求項４３】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴とするネットワーク保護方法。
【請求項４４】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴とするネットワーク保護方法。
【請求項４５】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのパケットのルーティングを、設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴とするネットワーク保護方法。
【請求項４６】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、関連する機器に対し機器認証を行う、またはやり直すことを特徴とするネットワーク保護方法。
【請求項４７】　請求項１６に記載のネットワーク監視方法からの警告の発生を受けて、データの暗号化を行う、または暗号化キーを再作成することを特徴とするネットワーク保護方法。
【請求項４８】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、
警告発生時の状態を収集する情報収集部と、
この収集された情報をユーザに通知する表示部とを具備し、
警告時に警告の内容と前記警告発生時の状態をユーザに通知することを特徴とするネットワーク装置。
【請求項４９】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、
警告発生時の状態を収集する情報収集部と、
公衆回線に接続された公衆回線通信部とを具備し、
警告時に警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴とするネットワーク装置。
【請求項５０】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、
警告発生時の状態を収集する情報収集部と、
情報を記録する記憶部とを具備し、
警告時に警告の内容と警告発生時の状態を記録することを特徴とするネットワーク装置。
【請求項５１】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、
警告に関連する機器の挙動または状態を収集する情報収集部と、
情報を記録する記憶部とを具備し、
警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴とするネットワーク装置。
【請求項５２】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、
他機器にサービスを提供するサービス処理部と、
条件によりサービスの提供の許可を行うサービス制御部とを具備し、
警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴とするネットワーク装置。
【請求項５３】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、
パケットのルーティングを行うルーティング部と、
ルーティングの設定を行うルーティング制御部とを具備し、
警告に関連した機器の何れかまたは全てからのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴とするネットワーク装置。
【請求項５４】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、

機器の認証機能を備えた機器認証部とを具備し、
関連する機器に対し機器認証を行う、またはやり直すことを特徴とするネットワーク装置。
【請求項５５】　請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、
データの暗号化を行う暗号部とを具備し、
データの暗号化を行う、または暗号化キーを再作成することを特徴とするネットワーク装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークのセキュリティを強化するネットワーク監視方法および装置に関し、特に、ＩＥＥＥ１３９４に代表されるバス型ネットワークにおけるセキュリティを強化するネットワーク監視方法および装置に関する。
【０００２】
【従来の技術】ＩＥＥＥ１３９４はシンプルな構成と高いパフォーマンスにより、家庭内ＬＡＮなど今後の様々な機器間接続手段として期待されている。１００Ｍｂｐｓ以上の転送速度、Ｉｓｏｃｈｒｏｎｏｕｓと呼ばれるマルチメディアデータ転送に適した転送方式、機器の接続を自動的に認識することで、ネットワークの稼働中に機器を追加、削除が可能な活線接続機能を備え、トゥリー型のネットワークを構成し広い用途に活用することが可能である。
【０００３】用途のひとつにカメラを用いた監視システムを構成することが考えられる。これは、高速な転送速度のために多量の映像等のデータを伝送することが可能になるためである。
【０００４】従来の監視システムの場合、監視に必要な数のアナログ出力カメラと、それと同数のビデオキャプチャボード等のＡ／Ｄ変換機構とを必要とし、また、カメラとビデオキャプチャボードとの接続に一本のケーブルを必要とし、カメラ台数と同じ本数のケーブルを引き回す必要があった。
【０００５】一方、ＩＥＥＥ１３９４を利用した監視システムの場合、監視に必要な数のＩＥＥＥ１３９４対応デジタル出力カメラに対し、監視装置として受信、記録のためのパソコンを最低ひとつ接続するだけで済み、またトゥリー型のネットワークを構成することにより、少ないケーブル本数で監視システムを構成することが可能となった。
【０００６】
【発明が解決しようとする課題】しかし、このような従来のＩＥＥＥ１３９４は、バス型ネットワークであり、送出されたパケットは基本的にバス上の全てのノードに届く。これにより、本来パケットを受信する必要の無い機器にパケットを盗聴される可能性があるという問題があった。
【０００７】また、バス上の全てのノードにパケットが届くことが前程とされているため、パケット上のソースＩＤの記述を確認する以外にパケットを送出したノードを特定する機構が無く、パケット上のソースＩＤの記述を偽られるという問題があった。
【０００８】ＩＥＥＥ１３９４を用いて監視システムを構築する場合、制御コマンドや秘匿性の高い情報など重要なパケットについて、その送出ノードおよび受信ノードが信用できる機器であることが保障されていることが望ましい。
【０００９】しかし上記問題はパケットの送受信に関わる機器の特定を妨げ、機器のなりすましを可能にするため、監視システムのセキュリティレベルを下げることになる。
【００１０】本発明はこのような問題を解決するためになされたもので、機器のなりすましを発見並びに対策する方法および装置を提供するものである。
【００１１】
【課題を解決するための手段】本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。
【００１２】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記記憶されたトポロジ情報と、前記記憶された応答時間との整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。
【００１３】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、パケットを受信したポートを識別し、受信パケットのソースＩＤを識別し、前記記憶されたトポロジ情報と、前記識別されたポートと前記識別されたソースＩＤの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。
【００１４】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記ネットワークのバスの状態が、ｇｒａｎｔ状態からｄａｔａ ｐｒｅｆｉｘ状態に変化するまでの時間を測定し、受信パケットのソースＩＤを識別し、前記記憶されたトポロジ情報と、前記記憶された応答時間と前記測定された時間と前記識別されたソースＩＤの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見

することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１５】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記ネットワークのバスの状態が、ｄａｔａ　ｅｎｄ状態からｒｅｑｕｅｓｔ状態に変化するまでの時間を測定し、受信パケットのソースＩＤを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースＩＤとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１６】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定し、受信パケットのソースＩＤを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースＩＤとの組み合わせとの整合性を判断することで、がネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１７】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、連続してパケットを受信した場合に、この受信した各パケットのソースＩＤとその受信順番を識別し、前記記憶されたトポロジ情報と、前記受信したパケットのソースＩＤと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１８】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、ＡＣＫとデータパケットを連続して受信した場合に、この受信した各パケットのソースＩＤとその受信順番を識別し、前記記憶されたトポロジ情報と、前記受信したパケットのソースＩＤと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１９】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定し、受信ＡＣＫパケットのソースノードを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたＡＣＫパケットのソースノードとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００２０】また、上記ネットワーク監視方法は、受信パケットのソースＩＤを識別し、この識別されたソースＩＤがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、前記ソースＩＤと前記ルーティングテーブルとが矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００２１】また、上記ネットワーク監視方法は、バスリセットをトリガとして、判断に使用する情報の収集を開始することを特徴としている。これにより、なりすまされている機器となりすましを行っている機器の候補が、少ない情報収集回数で判別できることとなる。

【００２２】また、上記ネットワーク監視方法において、矛盾を発見した場合に、前記パケットを破棄しても良い。また、矛盾を発見した場合に、前記パケットを破壊しても良い。あるいは、矛盾を発見した場合に、バスリセットを発生させても良い。これにより、なりすましが行なわれていた場合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【００２３】また、上記ネットワーク監視方法において、矛盾を発見した場合に、警告を発生しても良い。これにより、なりすましが行なわれている可能性を上位レイヤや他の機器に知らせることができ、他機器あるいはユーザに注意を促すことができることとなる。

【００２４】さらに、上記ネットワーク監視方法は、矛盾を発見した場合に、ポートを切り離しても良い。これにより、なりすましを行っている機器の候補をバスから強制的に排除することができることとなる。

【００２５】さらに、本発明のネットワーク監視装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することを特徴としている。この構成により、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００２６】また、本発明のネットワーク監視装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、前記トポロジ記憶部に記憶

されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間との整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。この構成により、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００２７】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、パケットを受信したポートを識別するポート識別部と、前記受信パケットのソースＩＤを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記ポート識別部に識別されたポートと前記ソース識別部に識別されたソースＩＤの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００２８】また、本発明のネットワーク監視装置は、複数のポータルを持つブリッジを含むネットワーク監視装置において、前記ブリッジが、ルーティング情報を記憶するルーティング記憶部と、パケットを受信したポータルを識別するポータル識別部と、前記受信パケットのソースＩＤを識別するソース識別部と、前記ルーティング記憶部に記憶されたルーティング情報と、前記ポータル識別部で識別されたポータルと前記ソース識別部で識別されたソースＩＤの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００２９】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がｇｒａｎｔ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースＩＤを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別された前記ソースＩＤの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００３０】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がｄａｔａ　ｅｎｄ状態からｒｅｑｕｅｓｔ状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースＩＤを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソースＩＤとの組み合わせの情報の整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００３１】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースＩＤを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソースＩＤの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００３２】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、パケットの連続を受信した場合に、それぞれのパケットのソースＩＤとその受信順番を識別するソース順番識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記ソース順番識別部で識別されたソースＩＤとその受信順番との整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００３３】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワ

ーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、ＡＣＫとデータパケットの連続を受信した場合に、それぞれのパケットのソースＩＤとその受信順番を識別するＡＣＫソース順番識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記ＡＣＫソース識別部で識別されたソースＩＤとその受信順番との整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００３４】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がｄａｔａ　ｅｎｄ状態からｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでの時間を測定する時間測定部と、受信ＡＣＫパケットのソースノードを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたＡＣＫパケットの前記ソースノードの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００３５】上記のネットワーク監視装置は、パケットのソースＩＤを識別するソース識別部と、ブリッジのルーティングテーブルを確認するルーティングテーブル確認部と、前記ソース識別部で識別されたソースＩＤと、前記ルーティングテーブル確認部で確認されたブリッジの前記ルーティングテーブルとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００３６】上記のネットワーク監視装置は、バスリセットをトリガとして、前記判断部で使用する情報の収集を開始することを特徴としている。これにより、なりすまされている機器となりすましを行っている機器の候補が少ない情報収集回数で判別できることとなる。

【００３７】上記のネットワーク監視装置において、矛盾を発見した場合に、前記パケットを破棄するパケット破棄処理部を具備しても良い。また、矛盾を発見した場合に、前記パケットを破壊するパケット破壊処理部を具備しても良い。あるいは、矛盾を発見した場合に、バスリセットを発生させるバスリセット発生処理部を具備しても良い。これにより、なりすましが行なわれていた場合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【００３８】上記のネットワーク監視装置において、矛盾を発見した場合に、警告を発生する警告発生処理部を具備しても良い。これにより、なりすましが行なわれている可能性を上位レイヤや他の機器に知らせることができ、他機器あるいはユーザに注意を促すことができることになる。

【００３９】上記のネットワーク監視装置において、矛盾を発見した場合に、ポートを切り離すポート接続制御処理部を具備しても良い。これにより、なりすましを行っている機器の候補をバスから強制的に排除することができることとなる。

【００４０】さらに、本発明のリピート方法は、ネットワークのトポロジ情報を記憶し、パケットのデスティネイションＩＤを識別し、前記トポロジ情報と前記デスティネイションＩＤの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピートするポートと、ダミー情報をリピートするポートとを決定することを特徴としている。これにより、なりすましや盗聴が行なわれていた場合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【００４１】また、上記のリピート方法において、バスリセットをトリガとして、前記情報の収集を開始しても良い。これにより、なりすましや盗聴が行なわれていた場合に少ない情報収集回数で、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【００４２】また、本発明のリピータ装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、パケットのデスティネイションＩＤを識別するデスティネイション識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と前記デスティネイション識別部で識別されたデスティネイションＩＤの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピートするポートと、ダミー情報をリピートするポートとを決定するポート制御部とを具備することを特徴としている。これにより、なりすましや盗聴が行なわれていた場合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【００４３】また、上記リピータ装置において、バスリセットをトリガとして、前記情報の収集を開始することを特徴としている。これにより、なりすましや盗聴が行なわれていた場合に少ない情報収集回数で、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【００４４】本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態をユーザに通知することを特徴としている。これにより、ユーザに速やかに、なりすましが行なわれている可能性を示すことができることとな

る。
【００４５】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴としている。これにより、遠隔地のユーザに速やかに、なりすましが行なわれている可能性を示すことができることとなる。
【００４６】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を記録することを特徴としている。これにより、なりすましの証拠とその時の状況を保存することができることとなる。
【００４７】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴としている。これにより、不正な機器について継続的に監視を行うことができることとなる。
【００４８】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴としている。これにより、不正な機器に提供するサービスを、通常と異なるものにすることができることとなる。
【００４９】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのパケットのルーティングを、設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴としている。これにより、不正な機器の通信の扱いを、通常と異なるものにすることができることとなる。
【００５０】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、関連する機器に対し機器認証を行う、またはやり直すことを特徴としている。これにより、不正の疑いのある機器が発見された場合に、不正な機器と正常な機器との確認ができることとなる。
【００５１】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、データの暗号化を行う、または暗号化キーを再作成することを特徴としている。これにより、不正の疑いのある機器が発見された場合に、セキュリティを厳しくすることができることとなる。
【００５２】本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告発生時の状態を収集する情報収集部と、この収集された情報をユーザに通知する表示部とを具備し、警告時に警告の内容と前記警告発生時の状態をユーザに通知することを特徴としている。これにより、ユーザに速やかに、なりすましが行なわれている可能性を示すことができることになる。
【００５３】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告発生時の状態を収集する情報収集部と、公衆回線に接続された公衆回線通信部とを具備し、警告時に警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴としている。これにより、遠隔地のユーザに速やかに、なりすましが行なわれている可能性を示すことができることとなる。
【００５４】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告発生時の状態を収集する情報収集部と、情報を記録する記憶部とを具備し、警告時に警告の内容と警告発生時の状態を記録することを特徴としている。これにより、なりすましの証拠とその時の状況を保存することができることとなる。
【００５５】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告に関連する機器の挙動または状態を収集する情報収集部と、情報を記録する記憶部とを具備し、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴としている。これにより、不正な機器について継続的に監視を行うことができることとなる。
【００５６】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、他機器にサービスを提供するサービス処理部と、条件によりサービスの提供の許可を行うサービス制御部とを具備し、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴としている。これにより、不正な機器に提供するサービスを、通常と異なるものにすることができることとなる。
【００５７】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、パケットのルーティングを行うルーティング部と、ルーティングの設定を行うルーティング制御部とを具備し、警告に関連した機器の何れかまたは全てからのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴としている。これにより、不正な機器の通信の扱いを、通常と異なるものにすることができることとなる。
【００５８】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、機器の認証機能を備えた機器認証部とを具備し、関連する機器に対し機器認証を行う、またはやり直すことを特徴としている。これにより、不正の疑いのある機器が発見された場合に、不正な機器と正常な機器との確認

ができることとなる。
【００５９】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、データの暗号化を行う暗号部とを具備し、データの暗号化を行う、または暗号化キーを再作成することを特徴としている。これにより、不正の疑いのある機器が発見された場合に、セキュリティを厳しくすることができることとなる。
【００６０】
【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。尚、全ての図面において、同様な構成要素は同じ参照記号および符号を用いて示してある。
（第１の実施の形態）
【００６１】図１に示すように、本発明の第１の実施の形態のネットワーク監視装置１は、送受信部５と、トポロジ記憶部６と、応答時間記憶部７と、判断部８と、各種処理部９とを備えている。本実施の形態において、送受信部５はポートＰ０、ポートＰ１、ポートＰ２の三ポートを有するものとするが、これに限定されるものでは無い。ポートＰ０～Ｐ２はそれぞれバス１０に接続されている。
【００６２】トポロジ記憶部６は、送受信部５を介してネットワークのトポロジ情報を収集し、記憶するものである。応答時間記憶部７は、送受信部５を介してネットワーク上のノードに応答検査コマンドであるｐｉｎｇを実行し、ネットワーク監視装置１とその他のノードとの間のｐｉｎｇに対する応答時間（以下、「ｐｉｎｇ時間」と呼ぶ）を記憶するものである。ｐｉｎｇを行う順番は、どのようなものでも構わない。判断部８は、トポロジ記憶部６に記憶されたトポロジ情報と、応答時間記憶部７に記憶されたｐｉｎｇ時間情報とを比較し、矛盾が存在するかどうかを判断するものである。各種処理部９は、判断部８で、矛盾が存在すると判断された場合、後述する各種処理を行うものである。
【００６３】上記のトポロジ情報の収集およびｐｉｎｇの実施は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。
【００６４】このように構成されたネットワーク監視装置１の動作を以下に説明する。
【００６５】始めに、ネットワークのトポロジ情報が送受信部５を介して収集され、トポロジ記憶部６に記憶される。次に、応答時間記憶部７により、送受信部５を介してネットワーク上のノードにｐｉｎｇが実行され、ネットワーク監視装置１とその他のノードとの間のｐｉｎｇ時間が記憶される。判断部８により、トポロジ記憶部６に記憶されたトポロジ情報と、応答時間記憶部７に記憶されたｐｉｎｇ時間情報とが比較され、矛盾が存在するかどうかが判断される。矛盾が存在すると判断された場合、各種処理部９により各種処理が行なわれる。
【００６６】図２に示すネットワークを例にして、本実施の形態のネットワーク監視装置１の判断部８による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置１からなる。ＩＤ＝０のノード２０１のｐｉｎｇ時間はＩＤ＝２のノード２０３のｐｉｎｇ時間よりも長いはずであり、その差は（ＰＨＹ遅延＋ケーブル遅延）に等しいはずである。この条件を満たしていない場合、判断部８は、トポロジ情報記憶部６に記憶されているトポロジ情報と、ｐｉｎｇ時間情報との間に矛盾が存在すると判断する。すなわち、ＩＤ＝０のノード２０１またはＩＤ＝２のノード２０３は、「他のノードに、なりすまされている」と考えられる。これをネットワーク全体に行うことにより、ネットワーク上のノードを正常なノードと不正なノードに判別することが可能である。以後、「不正なノード」とは、「なりすましを行っているノード」、「なりすましが行なわれているノード」のうちの何れかまたは全てを示す。
【００６７】また、例えばＩＤ＝２のノード２０３のｐｉｎｇ時間とＩＤ＝５のノード２０５のｐｉｎｇ時間とが等しかった場合、ＩＤ＝５のノード２０５がＩＤ＝２のノード２０３になりすましを行っている可能性があることが解る。
【００６８】以上のように、本発明の第１の実施の形態のネットワーク監視装置１は、送受信部５と、この送受信部５を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部６と、ｐｉｎｇを実行して、得られたｐｉｎｇ時間を記憶する応答時間記憶部７と、トポロジ記憶部６に記憶されたトポロジ情報と、応答時間記憶部７に記憶されたｐｉｎｇ時間情報とを比較し、矛盾が存在するかどうかを判断する判断部８と、各種処理部９とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補を発見することができる。
【００６９】各種処理部９が行う処理としては、以下のものが考えられる。
【００７０】各種処理部９は、判断部８で矛盾が発見された場合にパケットを破棄するパケット破棄処理部（図示無し）を有しても良い。各種処理部９のパケット破棄処理部は、不正なノードから送出されたパケットを破棄するように送受信部５を制御する。パケットを破棄するとは、受信したパケットを上位層に渡さないことと、受信したパケットをそのままリピートせずにダミーや一部を書き換え無害にしたパケットをリピートの替わりに送出することを示す。
【００７１】また、各種処理部９のパケット破棄処理部は、不正なノードに対し、送出されたパケットを全て破

棄させるようにしても良い。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。さらに、ネットワーク監視装置１よりも下流に存在するノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【００７２】あるいは、各種処理部９は、判断部８で矛盾が発見された場合にパケットを破壊するパケット破壊処理部（図示無し）を有しても良い。各種処理部９のパケット破壊処理部は、不正なノードから送出されたパケットを破壊するように、送受信部５を制御する。パケットを破壊するとは、受信したパケットを上位層に渡さないことと、パケットがバス上に存在する場合でも関係なくバスをドライブすることを示す。ここで、ドライブする状態としては、パケットデータ状態と衝突する状態であり、例えば、ＩＤＯＬ、ＴＸ＿ＤＡＴＡ＿ＥＮＤ、ＴＸ＿ＤＡＴＡ＿ＰＲＥＦＩＸ、ＴＸ＿ＲＥＱＵＥＳＴ、およびＢＵＳ＿ＲＥＳＥＴ等がある。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。さらに、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【００７３】あるいは、各種処理部９は、判断部８で矛盾が発見された場合にバスリセットを発生させるバスリセット発生処理部（図示無し）を有しても良い。各種処理部９のバスリセット発生処理部は、バスリセットを発生させるように送受信部５を制御する。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することもできる。

【００７４】あるいは、各種処理部９は、判断部８で矛盾が発見された場合に警告を発生する警告発生処理部（図示無し）を有しても良い。各種処理部９の警告発生処理部が発生する警告はネットワーク監視装置１の上位層に対して出されても良いし、送受信部５を介してネットワーク上の他のノードに出されても良い。なりすまされていることを報告するという点からなりすまされているノードに警告しても良い。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードが存在することを知ることができる。また、ネットワーク上のノードが、不正の疑いのあるノードが存在することを知ることができる。さらに、ネットワーク上のノードが、なりすましをされているということを知ることができる。

【００７５】あるいは、各種処理部９は、判断部８で矛盾が発見された場合にポートを切り離すポート接続制御処理部（図示無し）を有しても良い。各種処理部９のポート接続制御処理部は、ポートを使用しないように送受信部５を制御する。この時使用を停止するポートは不正なノードに繋がっているポートである。

【００７６】図２の例で言うと、なりすましを行っているのがＩＤ＝５のノード２０５であった場合、ポートＰ１の機能を停止させることで、ＩＤ＝５のノード２０５をバスに参加させないことが可能である。これにより不正の疑いのあるノードをバスから排除することができる。

【００７７】このように、各種処理部９は、矛盾を発見した場合に、なりすましで送出されたパケット等を破棄、破壊等をすることで、なりすましによるトランザクションの完了を防げ、さらに、なりすましの可能性を警告することで、他の機器あるいはユーザに注意を促すことが可能である。また、各種処理部９は、矛盾を発見した場合に、なりすまし機器を切り離し、バスに参加させないことで、なりすましを防止することができる。

（第２の実施の形態）

【００７８】図３は、本発明の第２の実施の形態のネットワーク監視方法を示すフローチャートを示す。同図に示すように、ステップＳ１０１において、ネットワークのトポロジ情報を獲得する。ステップＳ１０２において、ネットワーク上のノードについてｐｉｎｇを実行し、ｐｉｎｇ時間を獲得する。ステップＳ１０３において、ステップＳ１０１で獲得したトポロジ情報とステップＳ１０２で獲得したｐｉｎｇ時間を比較し、矛盾が存在するかどうかを判断する。矛盾が存在しなかった場合、ステップＳ１０４へ進み、バスリセットの発生を待機する。矛盾が存在した場合、ステップＳ１０５に進み、後述する各種処理を行う。ステップＳ１０５の各種処理が終了した後は、ステップＳ１０４へ進む。ステップＳ１０４において、バスリセットが検出された場合、ステップＳ１０１へ戻る。

【００７９】図２に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップＳ１０３における判断の方法を説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置１からなる。ＩＤ＝０のノード２０１のｐｉｎｇ時間はＩＤ＝２のノード２０３のｐｉｎｇ時間よりも長いはずであり、その差は（ＰＨＹ遅延＋ケーブル遅延）に等しいはずである。この条件を満たしていない場合、ステップＳ１０３で、ステップＳ１０１で獲得したトポロジ情報と、ステップＳ１０２で獲得したｐｉｎｇ時間情報との間に矛盾が存在すると判断する。すなわち、ＩＤ＝０のノード２０１またはＩＤ＝２のノード２０３は、「他のノードに、なりすまされている」と考えられる。これをネットワーク全体に行うことにより、ネットワーク上のノードを、正常なノードと不正なノードに判別することが可能である。

【００８０】また、例えばＩＤ＝２のノード２０３のｐｉｎｇ時間と、ＩＤ＝５のノード２０５のｐｉｎｇ時間

とが等しかった場合、ＩＤ＝５のノード２０５がＩＤ＝２のノード２０３になりすましを行っている可能性があることが解る。

【００８１】以上のように、本発明の第２実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、ｐｉｎｇを実行して、得られたｐｉｎｇ時間を記憶し、記憶されたトポロジ情報と、記憶されたｐｉｎｇ時間との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

【００８２】ステップＳ１０５で行なわれる各種処理としては、以下のものが考えられる。

【００８３】ステップＳ１０３で矛盾が発見された場合に、ステップＳ１０５において、不正なノードから送出されたパケットを破棄しても良い。パケットを破棄するとは、受信したパケットを上位層に渡さないことと、受信したパケットをそのままリピートせずにダミーや一部を書き換え無害にしたパケットをリピートの替わりに送出することを示す。

【００８４】また、ステップＳ１０５において、不正なノードに対し、送出されたパケットを全て破棄させるようにしても良い。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク監視装置１よりも下流に存在するノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【００８５】あるいは、ステップＳ１０３で矛盾が発見された場合に、ステップＳ１０５において、不正なノードから送出されたパケットを破壊しても良い。パケットを破壊するとは、受信したパケットを上位層に渡さないことと、パケットがバス上に存在する場合でも関係なくバスをドライブすることを示す。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【００８６】あるいは、ステップＳ１０３で矛盾が発見された場合に、ステップＳ１０５において、バスリセットを発生させても良い。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【００８７】あるいは、ステップＳ１０３で矛盾が発見された場合に、ステップＳ１０５において、警告を発生しても良い。警告は上位層に対して出されても良いし、ネットワーク上の他のノードに出されても良い。なりすまされていることを報告するという点から、なりすまされているノードに警告しても良い。これによりネットワーク監視装置１の上位層が、不正の疑いのあるノードが存在することを知ることができる。また、ネットワーク上のノードが、不正の疑いのあるノードが存在することを知ることができる。また、ネットワーク上のノードが、なりすましをされているということを知ることができる。

【００８８】あるいは、ステップＳ１０３で矛盾が発見された場合に、ステップＳ１０５において、ポートを切り離し、ポートの使用を停止しても良い。この時使用を停止するポートは不正なノードに繋がっているポートである。

【００８９】図２の例で言うと、なりすましを行っているのがＩＤ＝５のノード２０５であった場合、ポートＰ１の機能を停止させることで、ＩＤ＝５のノード２０５をバスに参加させないことが可能である。これにより不正の疑いのあるノードをバスから排除することができる。

【００９０】このように、ステップＳ１０３で矛盾を発見した場合に、ステップＳ１０５における各種処理において、なりすましで送出されたパケット等を破棄、破壊等をすることで、なりすましによるトランザクションの完了を防げ、さらに、なりすましの可能性を警告することで、他の機器あるいはユーザに注意を促すことが可能である。また、各種処理部９は、矛盾を発見した場合に、なりすまし機器を切り離し、バスに参加させないことで、なりすましを防止することができる。

（第３の実施の形態）

【００９１】図４は、本発明の第３の実施の形態のネットワーク監視装置２１の概略ブロック図を示す。これは上記第１の実施の形態とは、応答時間記憶部７の替わりに、ソース識別部１１を設けた点が相違している。第１の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【００９２】ソース識別部１１は、送受信部５を介してパケットを受信した際に、そのパケットのソースＩＤとパケットを受信したポートを識別するものである。

【００９３】以下に、本実施の形態のネットワーク監視装置２１の動作を説明する。

【００９４】始めに、ネットワークのトポロジ情報が送受信部５を介して収集され、トポロジ記憶部６に記憶される。次に、ソース識別部１１により、パケットが受信され、パケットのソースＩＤとパケットを受信したポートが識別される。判断部８により、トポロジ記憶部６に記憶されたトポロジ情報と、ソース識別部１１が識別したパケットのソースＩＤとパケットを受信したポートとが比較され、矛盾が存在するかどうかが判断される。矛盾が存在すると判断された場合、各種処理部９により、上記第１の実施の形態と同様な各種処理が行われる。こ

れにより、本実施の形態においても第１の実施の形態と同様な効果が得られる。

【００９５】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【００９６】図２に示すネットワークを例にして、本実施の形態のネットワーク監視装置２１の判断部８による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置２１からなる。ソースＩＤがＩＤ＝０のノード２０１から送出されたパケットは、ネットワークトポロジ上、必ずポートＰ０を介して受信されるはずである。これがポートＰ０以外のポートを介して受信された場合、ＩＤ＝０のノード２０１は他のノードになりすまされていると考えられる。

【００９７】以上のように、本発明の第２の実施の形態のネットワーク監視装置２１は、送受信部５と、この送受信部５を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部６と、送受信部５を介してパケットを受信した際に、そのパケットのソースＩＤとパケットを受信したポートを識別するソース識別部１１と、トポロジ記憶部６に記憶されたトポロジ情報と、応答時間記憶部７に記憶されたｐｉｎｇ時間情報とを比較し、矛盾が存在するかどうかを判断する判断部８と、各種処理部９とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードが接続されているポートを発見することができる。

（第４の実施の形態）

【００９８】図５は、本発明の第４の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第２の実施の形態とは、ステップＳ１０２およびＳ１０３の替わりに、ステップＳ１１１乃至ステップＳ１１３を設けた点が主に相違している。

【００９９】同図に示すように、ステップＳ１０１において、ネットワークのトポロジ情報を獲得する。次いでステップＳ１０４において、バスリセットの発生を待機する。ステップＳ１０４において、バスリセットが検出された場合、ステップＳ１０１へ戻り、検出されない場合はステップＳ１１１へ進む。ステップＳ１１１において、パケットの受信を待機する。ステップＳ１１１において、パケットが受信されない場合は、ステップＳ１０４へ戻り、パケットが受信された場合、ステップＳ１１２へ進む。

【０１００】ステップＳ１１２において、パケットを受信したポートとパケットのソースＩＤを識別する。次いでステップＳ１１３において、ステップＳ１０１で獲得したトポロジ情報とステップＳ１１２で識別したパケットのソースＩＤとパケットを受信したポートとを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップＳ１０５に進み、各種処理を行う。ステップＳ１０５における各種処理は、図３に示された上記第２の実施の形態におけるステップＳ１０５の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第２の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップＳ１０４へ戻る。ステップＳ１０５の各種処理が終了した後も、ステップＳ１０４へ戻る。

【０１０１】図２に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップＳ１１３における判断の方法を説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置２１からなる。ソースＩＤがＩＤ＝０のノード２０１から送出されたパケットは、ネットワークトポロジ上、必ずポートＰ０を介して受信されるはずである。これがポートＰ０以外のポートを介して受信された場合、ＩＤ＝０のノード２０１は他のノードになりすまされていると考えられる。

【０１０２】以上のように、本発明の第４の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、パケットを受信したポートを識別し、受信したパケットのソースＩＤを識別し、記憶されたトポロジ情報と、識別された記憶されたポートとソースＩＤの組み合わせとの整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードが接続されているポートとを発見することができる。

（第５の実施の形態）

【０１０３】図６は、本発明の第５の実施の形態のネットワーク監視装置３１の概略ブロック図を示す。これは上記第１の実施の形態とは、さらにソース識別部１１と時間測定部１２を設けた点が相違している。上記の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【０１０４】時間測定部１２は、送受信部５を介してバス上の状態が変化した時間を測定するものである。測定される時間については後述する。

【０１０５】以下に、本実施の形態のネットワーク監視装置３１の動作を説明する。

【０１０６】始めに、ネットワークのトポロジ情報が送受信部５を介して収集され、トポロジ記憶部６に記憶される。次に、応答時間記憶部７により、送受信部５を介してネットワーク上のノードにｐｉｎｇが実行され、ネットワーク監視装置３１とその他のノードとの間のｐｉｎｇ時間が記憶される。ここで、ｐｉｎｇを行う順番はどのようなものでも構わない。

【０１０７】次に、ソース識別部１１により、パケット

が受信され、パケットのソースＩＤとパケットを受信したポートが識別される。さらに、時間測定部１２により、送受信部５を介してバス上の状態が変化した時間が測定される。判断部８により、トポロジ記憶部６に記憶されたトポロジ情報と、応答時間記憶部７に記憶されたｐｉｎｇ時間情報と、ソース識別部１１に識別されたソースＩＤ情報と、時間測定部１２が測定したバス状態時間測定情報とが比較され、矛盾が存在するかどうかが判断される。矛盾が存在すると判断された場合、各種処理部９により、上記第１の実施の形態と同様な各種処理が行なわれる。これにより、本実施の形態においても第１の実施の形態と同様な効果が得られる。

【０１０８】上記のトポロジ情報の収集およびｐｉｎｇの実施は、設定された時間毎に行なわれても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行なわれても良い。バスリセット発生毎に行なわれるのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【０１０９】図２に示すネットワークを例にして、本実施の形態のネットワーク監視装置３１の判断部８による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置３１からなる。

【０１１０】ＩＤ＝０のノード２０１がパケットを送出する場合には、以下の手順を行う。最初に、パケットを送出するためにバスの利用権を得たい旨を、上流のバス状態をｒｅｑｕｅｓｔ状態にドライブすることにより知らせる。次に、ルートノード（この場合はＩＤ＝１０のノード２１０）がＩＤ＝０のノード２０１への経路のバス状態をｇｒａｎｔ状態にドライブする。ｇｒａｎｔ状態を検知したＩＤ＝０のノード２０１は、バスをｄａｔａ　ｐｒｅｆｉｘ状態にドライブし、パケットの送出を開始する。この時、ネットワーク監視装置３１から見た場合、バス状態がｇｒａｎｔ状態に変化してからｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでに、おおよそ下記の式（１）の時間が経過するはずである。

【０１１１】

ＰＨＹ遅延×４＋ケーブル遅延×４＋ｐｉｎｇ時間　　・・・式（１）

【０１１２】ソースＩＤ＝０のパケットを受信した時に、その直前のｇｒａｎｔ－ｄａｔａｐｒｅｆｉｘ間時間が上記の式（１）の値と異なる場合、そのパケットはＩＤ＝０のノード２０１が送出したものではないと考えられる。

【０１１３】また、その際のｇｒａｎｔ－ｄａｔａ　ｐｒｅｆｉｘ間時間が、下記の式（２）であった場合、この値はＩＤ＝２のノード２０３がパケット送出する場合の値と一致するため、ＩＤ＝２のノード２０３がＩＤ＝０のノード２０１になりすましていると考えられる。

【０１１４】

ＰＨＹ遅延×２＋ケーブル遅延×２＋ｐｉｎｇ時間　　・・・式（２）

時間測定部１２が測定する時間は、ｇｒａｎｔ－ｄａｔａ　ｐｒｅｆｉｘ間時以外にも、ｄａｔａ　ｅｎｄ－ｒｅｑｕｅｓｔ間時間、ｄａｔａ　ｅｎｄ－ｄａｔａ　ｐｒｅｆｉｘ間時間あるいは、ｄａｔａ　ｅｎｄ－ＡＣＫのｄａｔａ　ｐｒｅｆｉｘ間時間が考えられる。

【０１１５】また、これらはルートノードが正常であることを前程とした場合であり、ルートノードが不正なノードである可能性を考慮すると、ｒｅｑｕｅｓｔ－ｇｒａｎｔ間時間や、ｒｅｑｕｅｓｔ－ｄａｔａ　ｐｒｅｆｉｘ間時間も判断の材料となる。従って、時間測定部１２は、ｒｅｑｕｅｓｔ－ｇｒａｎｔ間時間または、ｒｅｑｕｅｓｔ－ｄａｔａ　ｐｒｅｆｉｘ間時間を測定しても良く、これにより、ルートノードが不正なノードである場合も同様な効果が得られることとなる。

【０１１６】以上のように、本発明の第５の実施の形態のネットワーク監視装置３１は、送受信部５と、この送受信部５を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部６と、ｐｉｎｇを実行して、得られたｐｉｎｇ時間を記憶する応答時間記憶部７と、送受信部５を介してパケットを受信した際に、そのパケットのソースＩＤとパケットを受信したポートを識別するソース識別部１１と、送受信部５を介してバス上の状態が変化した時間を測定する時間測定部１２と、トポロジ記憶部６に記憶されたトポロジ情報と、応答時間記憶部７に記憶されたｐｉｎｇ時間情報と、ソース識別部１１で識別されたソースＩＤと、時間測定部１２で測定された時間とを比較し、矛盾が存在するかどうかを判断する判断部８と、各種処理部９とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補を発見することができる。

（第６の実施の形態）

【０１１７】図７は、本発明の第６の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第２の実施の形態とは、ステップＳ１０３の替わりに、ステップＳ１２１乃至ステップＳ１２３を設けた点が主に相違している。

【０１１８】同図に示すように、ステップＳ１０１において、ネットワークのトポロジ情報を獲得する。次いでステップＳ１０２において、ネットワーク上のノードについてｐｉｎｇを実行し、ｐｉｎｇ時間を獲得する。次いで、ステップＳ１０４において、バスリセットの発生を待機する。ステップＳ１０４において、バスリセットが検出されなかった場合、ステップＳ１０１へ戻り、検出された場合は、ステップＳ１２１へ進む。

【０１１９】ステップＳ１２１において、バス状態の変

化時間を測定する。ここで測定される時間については後述する。次いでステップＳ１２２において、パケットを受信したポートとパケットのソースＩＤを識別する。次いでステップＳ１２３において、ステップＳ１０１で獲得したトポロジ情報と、ステップＳ１０２で獲得した応答時間と、ステップＳ１２１で測定したバス状態の変化時間情報と、ステップＳ１２２で識別したパケットのソースＩＤ情報とが比較され、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップＳ１０５で各種処理を行う。ステップＳ１０５における各種処理は、図３に示された上記第２の実施の形態におけるステップＳ１０５の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第２の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップＳ１０４へ戻る。ステップＳ１０５の各種処理が終了した後も、ステップＳ１０４へ戻る。

【０１２０】図２に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップＳ１２３における判断の方法を説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置３１からなる。

【０１２１】ＩＤ＝０のノード２０１がパケットを送出する場合には、以下の手順を行う。最初にパケットを送出するためにバスの利用権を得たい旨を、上流のバス状態をｒｅｑｕｅｓｔ状態にドライブすることで知らせる。次に、ルートノード（この場合はＩＤ＝１０のノード２１０）がＩＤ＝０のノード２０１への経路のバス状態をｇｒａｎｔ状態にドライブする。ｇｒａｎｔ状態を検知したＩＤ＝０のノード２０１は、バスをｄａｔａ　ｐｒｅｆｉｘ状態にドライブし、パケットの送出を開始する。この時、ネットワーク監視装置３１から見た場合、バス状態がｇｒａｎｔ状態に変化してからｄａｔａ　ｐｒｅｆｉｘ状態に変化するまでに、おおよそ下記の式（３）の時間が経過するはずである。

【０１２２】

PHY遅延×４＋ケーブル遅延×４＋ｐｉｎｇ時間　　・・・式（３）

【０１２３】ソースＩＤ＝０のパケットを受信した時に、その直前のｇｒａｎｔ－ｄａｔａｐｒｅｆｉｘ間時間が上記の式（３）の値と異なる場合、そのパケットはＩＤ＝０のノード２０１が送出したものではないと考えられる。

【０１２４】また、その際のｇｒａｎｔ－ｄａｔａ　ｐｒｅｆｉｘ間時間が下記の式（４）であった場合、この値はＩＤ＝２のノード２０３がパケット送出する場合の値と一致するため、ＩＤ＝２のノード２０３がＩＤ＝０のノード２０１になりすましていると考えられる。

【０１２５】

PHY遅延×２＋ケーブル遅延×２＋ｐｉｎｇ時間　　・・・式（４）

【０１２６】ステップＳ１２１で測定する時間は、ｇｒａｎｔ－ｄａｔａ　ｐｒｅｆｉｘ間時以外にも、ｄａｔａ　ｅｎｄ－ｒｅｑｕｅｓｔ間時間、ｄａｔａ　ｅｎｄ－ｄａｔａ　ｐｒｅｆｉｘ間時間あるいは、ｄａｔａ　ｅｎｄ－ＡＣＫのｄａｔａｐｒｅｆｉｘ間時間が考えられる。

【０１２７】また、これらはルートノードが正常であることを前程とした場合であり、ルートノードが不正なノードである可能性を考慮すると、ｒｅｑｕｅｓｔ－ｇｒａｎｔ間時間や、ｒｅｑｕｅｓｔ－ｄａｔａ　ｐｒｅｆｉｘ間時間も判断の材料となる。従って、ステップＳ１２１では、ｒｅｑｕｅｓｔ－ｇｒａｎｔ間時間または、ｒｅｑｕｅｓｔ－ｄａｔａ　ｐｒｅｆｉｘ間時間を測定しても良く、これにより、ルートノードが不正なノードである場合も同様な効果が得られることとなる。

【０１２８】以上のように、本発明の第６の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、ｐｉｎｇを実行して、得られたｐｉｎｇ時間を記憶し、パケットを受信したポートを識別し、受信したパケットのソースＩＤを識別し、バス上の状態が変化した時間を測定し、記憶されたトポロジ情報と、記憶されたｐｉｎｇ時間と、識別された記憶されたソースＩＤと、測定された時間との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

（第７の実施の形態）

【０１２９】図８は、本発明の第７の実施の形態のネットワーク監視装置４１の概略ブロック図を示す。これは上記第１の実施の形態とは、応答時間記憶部７の替わりに、ソース順番識別部１３を設けた点が相違している。第１の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【０１３０】ソース順番識別部１３は、連続したパケットを受信した際に、受信したパケットのソースＩＤとその受信順番を識別するものである。

【０１３１】以下に、本実施の形態のネットワーク監視装置４１の動作を説明する。

【０１３２】始めに、ネットワークのトポロジ情報が送受信部５を介して収集され、トポロジ記憶部６に記憶される。次に、ソース順番識別部１３により、連続したパケットが受信された場合に、その連続したパケットのソースＩＤとその受信順番が識別される。判断部８により、トポロジ記憶部６に記憶されたトポロジ情報と、ソース順番識別部１３識別されたパケットのソースＩＤとその受信順番とが比較され、矛盾が存在するかどうかが判断される。矛盾が存在すると判断された場合、各種処理部９により、上記第１の実施の形態と同様な各種処理

が行なわれる。これにより、本実施の形態においても第１の実施の形態と同様な効果が得られる。

【０１３３】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【０１３４】図２に示すネットワークを例にして、本実施の形態のネットワーク監視装置４１の判断部８による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置４１からなる。ＩＤ＝６のノード２０６とＩＤ＝７のノード２０７とＩＤ＝９のノード２０９から連続したパケットが送出された場合、そのパケットの順番は、ＩＤ＝６のノード２０６、ＩＤ＝７のノード２０７、ＩＤ＝９のノード２０９であるはずである。これ以外の順番の連続パケットが観測された場合、矛盾が存在することになる。

【０１３５】また、その矛盾した順番が、ＩＤ＝７のノード２０７、ＩＤ＝９のノード２０９、ＩＤ＝６のノード２０６であった場合、ＩＤ＝７のノード２０７とＩＤ＝９のノード２０９の順番は正しいが、ＩＤ＝６のノード２０６の順番が不自然であることが解る。

【０１３６】ここから、ＩＤ＝６のノード２０６がなりすまされている可能性があることが解り、またトポロジ情報から、なりすましを行っているノードは、ＩＤ＝９のノード２０６よりもルートよりのノード、図２の場合はＩＤ＝１０のノード２１０である可能性があることが解る。

【０１３７】以上のように、本発明の第７の実施の形態のネットワーク監視装置４１は、送受信部５と、この送受信部５を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部６と、連続したパケットを受信した際に、受信したパケットのソースＩＤとその受信順番を識別するソース順番識別部１３と、トポロジ記憶部６に記憶されたトポロジ情報と、ソース順番識別部１３で識別されたパケットのソースＩＤとその受信順番とを比較し、矛盾が存在するかどうかを判断する判断部８と、各種処理部９とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

（第８の実施の形態）

【０１３８】図９は、本発明の第８の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第２の実施の形態とは、ステップＳ１０２およびＳ１０３の替わりに、ステップＳ１３１乃至ステップＳ１３３を設けた点が主に相違している。

【０１３９】同図に示すように、ステップＳ１０１において、ネットワークのトポロジ情報を獲得する。次いでステップＳ１０４において、バスリセットの発生を待機する。ステップＳ１０４において、バスリセットが検出された場合、ステップＳ１０１へ戻り、検出されない場合はステップＳ１３１へ進む。ステップＳ１３１において、連続パケットの受信を待機する。ステップＳ１３１において、パケットが受信されない場合は、ステップＳ１０４へ戻り、パケットが受信された場合、ステップＳ１３２へ進む。

【０１４０】ステップＳ１３２において、パケットを受信した順番とパケットのソースＩＤを識別する。次いでステップＳ１３３において、ステップＳ１０１で獲得したトポロジ情報とステップＳ１３２で識別したパケットのソースＩＤとパケットを受信した順番とを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップＳ１０５で各種処理を行う。ステップＳ１０５における各種処理は、図３に示された上記第２の実施の形態におけるステップＳ１０５の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第２の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップＳ１０４へ戻る。ステップＳ１０５の各種処理が終了した後も、ステップＳ１０４へ戻る。

【０１４１】図２に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップＳ１３３における判断の方法を説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置４１からなる。ＩＤ＝６のノード２０６とＩＤ＝７のノード２０７とＩＤ＝９のノード２０９から連続したパケットが送出された場合、そのパケットの順番は、ＩＤ＝６のノード２０６、ＩＤ＝７のノード２０７、ＩＤ＝９のノード２０９であるはずである。これ以外の順番の連続パケットが観測された場合、矛盾が存在することになる。

【０１４２】また、その矛盾した順番が、ＩＤ＝７のノード２０７、ＩＤ＝９のノード２０９、ＩＤ＝６のノード２０６であった場合、ＩＤ＝７のノード２０７とＩＤ＝９のノード２０９の順番は正しいが、ＩＤ＝６のノード２０６の順番が不自然であることが解る。

【０１４３】ここから、ＩＤ＝６のノード２０６がなりすまされている可能性があることが解り、またトポロジ情報から、なりすましを行っているノードは、ＩＤ＝９のノード２０６よりもルートよりのノード、図２の場合はＩＤ＝１０のノード２１０である可能性があることが解る。

【０１４４】以上のように、本発明の第８の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、連続したパケットを受信した際に、受信したパケットのソースＩＤとその受信順番を識別し、記憶されたトポロジ情報と、識別されたパケットのソースＩ

Dとその受信順番との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

(第９の実施の形態)

【０１４５】図１０は、本発明の第９の実施の形態のネットワーク監視装置５１の概略ブロック図を示す。これは上記第１の実施の形態とは、応答時間記憶部７の替わりに、ＡＣＫソース識別部１４を設けた点が相違している。第１の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【０１４６】ＡＣＫソース識別部１４は、ＡＣＫに連続したパケットを受信した際に、ＡＣＫとそれに連続したパケットのソースＩＤとその受信順番を識別するものである。

【０１４７】以下に、本実施の形態のネットワーク監視装置５１の動作を説明する。

【０１４８】始めに、ネットワークのトポロジ情報が送受信部５を介して収集され、トポロジ記憶部６に記憶される。次に、ＡＣＫソース順番識別部１４により、ＡＣＫに連続したパケットが受信され、ＡＣＫとそれに連続したパケットのソースＩＤとその受信順番が識別される。判断部８により、トポロジ記憶部６に記憶されたトポロジ情報と、ＡＣＫソース順番識別部１４に識別されたＡＣＫとパケットのソースＩＤとその受信順番とが比較され、矛盾が存在するかどうかが判断される。矛盾が存在すると判断された場合、各種処理部９により、上記第１の実施の形態と同様な各種処理が行なわれる。これにより、本実施の形態においても第１の実施の形態と同様な効果が得られる。

【０１４９】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【０１５０】図２に示すネットワークを例にして、本実施の形態のネットワーク監視装置５１の判断部８による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置５１からなる。

【０１５１】ＩＤ＝７のノード２０７から送出されたＡＣＫにパケットを連続できるのは、トポロジ上、ＩＤ＝９のノード２０９とＩＤ＝１０のノード２１０のみである。それ以外のソースＩＤを持つパケットが、ＩＤ＝７のノード２０７のＡＣＫに連続していた場合、矛盾が存在することになる。ＩＤ＝７のノード２０７のＡＣＫに、ソースＩＤがＩＤ＝６のノード２０６であるパケットが連続していた場合、ＩＤ＝６のノード２０６はなりすまされている可能性があることが解る。また、なりすましを行っているノードは、ＩＤ＝９のノード２０９またはＩＤ＝１０のノード２１０である可能性があることが解る。

【０１５２】以上のように、本発明の第９の実施の形態のネットワーク監視装置５１は、送受信部５と、この送受信部５を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部６と、ＡＣＫに連続したパケットを受信した際に、ＡＣＫとそれに連続したパケットのソースＩＤとその受信順番を識別するＡＣＫソース識別部１４と、トポロジ記憶部６に記憶されたトポロジ情報と、ＡＣＫソース識別部１４で識別されたパケットのソースＩＤとその受信順番とを比較し、矛盾が存在するかどうかを判断する判断部８と、各種処理部９とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補を発見することができる。

(第１０の実施の形態)

【０１５３】図１１は、本発明の第１０の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第２の実施の形態とは、ステップＳ１０２およびＳ１０３の替わりに、ステップＳ１４１乃至ステップＳ１４３を設けた点が主に相違している。

【０１５４】同図に示すように、ステップＳ１０１において、ネットワークのトポロジ情報を獲得する。次いでステップＳ１０４において、バスリセットの発生を待機する。ステップＳ１０４において、バスリセットが検出された場合、ステップＳ１０１へ戻り、検出されない場合はステップＳ１４１へ進む。ステップＳ１４１において、ＡＣＫに連続したパケットの受信を待機する。ステップＳ１４１において、パケットが受信されない場合は、ステップＳ１０４へ戻り、パケットが受信された場合、ステップＳ１４２へ進む。

【０１５５】ステップＳ１４２において、ＡＣＫとパケットのソースＩＤを識別する。次いでステップＳ１４３において、ステップＳ１０１で獲得したトポロジ情報とステップＳ１４２で識別したＡＣＫとパケットのソースＩＤとを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップＳ１０５に進み、各種処理を行う。ステップＳ１０５における各種処理は、図３に示された上記第２の実施の形態におけるステップＳ１０５の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第２の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップＳ１０４へ戻る。ステップＳ１０５の各種処理が終了した後も、ステップＳ１０４へ戻る。

【０１５６】図２に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップＳ１４３における判断の方法を説明する。同図に示すように、このネットワークは、ノード２０１～２１０とネットワーク監視装置５１からなる。

【0157】ID＝7のノード207から送出されたACKにパケットを連続できるのは、トポロジ上ID＝9のノード209とID＝10のノード210のみである。それ以外のソースIDを持つパケットが、ID＝7のノード207のACKに連続していた場合、矛盾が存在することになる。ID＝7のノード207のACKに、ソースIDがID＝6のノード206であるパケットが連続していた場合、ID＝6のノード206はなりすまされている可能性があることが解る。また、なりすましを行っているノードは、ID＝9のノード209またはID＝10のノード210である可能性があることが解る。

【0158】以上のように、本発明の第10の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、ACKに連続したパケットを受信した際に、受信したACKとそれに連続したパケットのソースIDとその受信順番を識別し、記憶されたトポロジ情報と、識別されたACKとパケットのソースIDとその受信順番との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

（第11の実施の形態）

【0159】図12は、本発明の第11の実施の形態のネットワーク監視装置61の概略ブロック図を示す。これは図6に示す上記第5の実施の形態とは、さらにルーティングテーブル確認部15を設けた点が相違している。上記の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【0160】ルーティングテーブル確認部15は、判断部8と送受信部5に接続され、判断部8で矛盾が存在しないと判断され、かつ判断部8を介して得られたソースIDが仮想ノードIDであった場合、ブリッジなどのネットワーク中継機器のルーティングテーブルを取得するものである。

【0161】以下に、本実施の形態のネットワーク監視装置61の動作を説明する。

【0162】始めに、ネットワークのトポロジ情報が送受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、応答時間記憶部7により、送受信部5を介してネットワーク上のノードにpingが実行され、ネットワーク監視装置61とその他のノードとの間のping時間が記憶される。ここで、pingを行う順番はどのようなものでも構わない。

【0163】次に、ソース識別部11により、パケットが受信され、パケットのソースIDとパケットを受信したポートが識別される。さらに、時間測定部12により、送受信部5を介してバス上の状態が変化した時間が測定される。判断部8により、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報と、ソース識別部11に識別されたソースID情報と、時間測定部12が測定したバス状態時間測定情報とが比較され、矛盾が存在するかどうかが判断される。矛盾が存在すると判断された場合、各種処理部9により、上記第1の実施の形態と同様な各種処理が行なわれる。これにより、本実施の形態においても第1の実施の形態と同様な効果が得られる。

【0164】上記のトポロジ情報の収集およびpingの実施は、設定された時間毎に行なわれても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行なわれても良い。バスリセット発生毎に行なわれるのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0165】また、ソースIDが仮想ノードIDであった場合、そのパケットを送出したノードはブリッジ、ルータ等のネットワーク中継機器である。矛盾が存在しないと判断され、かつソースIDが仮想ノードIDであった場合、ルーティングテーブル確認部15は、ネットワーク中継機器のルーティングテーブルを取得する。その後、判断部8は、ソース識別部11のソースID情報と、ルーティングテーブル確認部15のルーティングテーブル情報とを比較し、矛盾が存在するかどうかを判断する。矛盾が存在すると判断された場合、各種処理部9が処理を行う。尚、ルーティングテーブルをキャッシュしておくことで、毎回ルーティングテーブルを獲得に行く必要をなくしても良い。

【0166】以上のように、本発明の第11の実施の形態のネットワーク監視装置61は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、pingを実行して、得られたping時間を記憶する応答時間記憶部7と、送受信部5を介してパケットを受信した際に、そのパケットのソースIDとパケットを受信したポートを識別するソース識別部11と、送受信部5を介してバス上の状態が変化した時間を測定する時間測定部12と、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報と、ソース識別部11で識別されたソースIDと、時間測定部12で測定された時間とを比較し、矛盾が存在するかどうかを判断する判断部8と、判断部8で矛盾が存在しないと判断され、かつ判断部8を介して得られたソースIDが仮想ノードIDであった場合、ブリッジなどのネットワーク中継機器のルーティングテーブルを取得するルーティングテーブル確認部15と、各種処理部9とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

（第12の実施の形態）

【0167】図13は、本発明の第12の実施の形態のネットワーク監視方法を示すフローチャートを示す。こ

れは図７に示す上記第６の実施の形態とは、さらにステップＳ１５１乃至ステップＳ１５３を設けた点が相違している。

【０１６８】同図に示すように、ステップＳ１０１において、ネットワークのトポロジ情報を獲得する。次いでステップＳ１０２において、ネットワーク上のノードについてｐｉｎｇを実行し、ｐｉｎｇ時間を獲得する。次いで、ステップＳ１０４において、バスリセットの発生を待機する。ステップＳ１０４において、バスリセットが検出されなかった場合、ステップＳ１０１へ戻り、検出された場合は、ステップＳ１２１へ進む。

【０１６９】ステップＳ１２１において、バス状態の変化時間を測定する。次いでステップＳ１２２において、パケットを受信したポートとパケットのソースＩＤを識別する。次いでステップＳ１２３において、ステップＳ１０１で獲得したトポロジ情報と、ステップＳ１０２で獲得した応答時間と、ステップＳ１２１で測定したバス状態の変化時間情報と、ステップＳ１２２で識別したパケットのソースＩＤ情報とが比較され、矛盾が存在するかどうかを判断する。矛盾が存在しなかった場合は、ステップＳ１５１へ進み、ソースノードがブリッジであるか否かを判定する。ブリッジでなかった場合は、ステップＳ１０４へ戻り、ブリッジであった場合、ステップＳ１５２でルーティングテーブルを獲得する。ルーティングテーブルとパケットのソースＩＤを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップＳ１０５で各種処理を行う。ステップＳ１０５における各種処理は、図３に示された上記第２の実施の形態におけるステップＳ１０５の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第２の実施の形態と同様な効果が得られる。一方、矛盾が存在しなかった場合は、ステップＳ１０４へ戻る。ステップＳ１０５の各種処理が終了した後も、ステップＳ１０４へ戻る。

【０１７０】ここで、ブリッジとはルーティングテーブルと、パケットの中継機能を備えた機器を指す。尚、ルーティングテーブルをキャッシュしておくことで、毎回ルーティングテーブルを獲得に行く必要をなくしても良い。

【０１７１】以上のように、本発明の第１２の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、ｐｉｎｇを実行して、得られたｐｉｎｇ時間を記憶し、パケットを受信したポートを識別し、受信したパケットのソースＩＤを識別し、バス上の状態が変化した時間を測定し、記憶されたトポロジ情報と、記憶されたｐｉｎｇ時間と、識別された記憶されたソースＩＤと、測定された時間との整合性を判断し、識別されたソースＩＤがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、ソースＩＤとルーティングテーブルとが矛盾する場合を発見するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

（第１３の実施の形態）

【０１７２】図１４は、本発明の第１３の実施の形態のリピータ装置７１の概略ブロック図を示す。同図に示すように、本実施の形態のリピータ装置７１は、送受信部５と、トポロジ記憶部６と、デスティネイション識別部１６と、ポート制御部１７を備えている。第１の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【０１７３】デスティネイション識別部１６は、送受信部５がパケットを受信した際に、パケットのデスティネイションＩＤを識別するものである。ポート制御部１７は、トポロジ記憶部６に記憶されたトポロジ情報と、デスティネイション識別部１６で識別されたデスティネイションＩＤ情報とから、ポートの状態を判断し、パケットのリピートに関するポートの制御を行うものである。

【０１７４】以下に、本実施の形態のリピータ装置７１の動作を説明する。

【０１７５】始めに、ネットワークのトポロジ情報が送受信部５を介して収集され、トポロジ記憶部６に記憶される。次に、送受信部５によりパケットが受信されると、デスティネイション識別部１６により、パケットのデスティネイションＩＤが識別される。次に、ポート制御部１７により、トポロジ記憶部６に記憶されたネットワークのトポロジ情報と、デスティネイション識別部１６に識別されたデスティネイションＩＤ情報とから、ポートの状態が判断され、パケットのリピートに関するポートが制御される。ポート制御の方法については後述する。

【０１７６】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【０１７７】図２に示すネットワークを例にして、本実施の形態のリピータ装置７１のポート制御部１７におけるポート制御の方法を以下に説明する。同図に示すように、このネットワークは、ノード２０１～２１０とリピータ装置７１からなる。

【０１７８】パケットのデスティネイションＩＤが３であった場合、このパケットはＩＤ＝３のノード２０４が接続されているポートＰ２のみにリピートすれば、パケットの役割を果たすことができるため、それ以外のポート、ポートＰ０およびポートＰ１にはリピートする必要はない。

【０１７９】しかし、バスを占有していることを示すために、何らかのデータをドライブする必要はある。そこ

でポート制御部１７は以下のようにポートを制御する。
【０１８０】ポートＰ２は通常どおりにパケットのリピートを行う。パケットを受信したポートには通常どおりにリピートを行わない。ポートＰ０およびポートＰ１には、パケットと同サイズのダミーをリピートする。ダミーとしては、パケットのデータペイロード等重要と思われる部分を書き換えたもの、あるいは、あらかじめ用意してある無害なパケットが考えられ、またパケットでなくｄａｔａ　ｐｒｅｆｉｘを出しつづけても良い。
【０１８１】以上のように、本発明の第１３の実施の形態のリピータ装置は、送受信部５と、この送受信部５を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部６と、送受信部５がパケットを受信した際に、パケットのデスティネイションＩＤを識別するデスティネイション識別部１６と、トポロジ記憶部６に記憶されたトポロジ情報と、デスティネイション識別部１６で識別されたデスティネイションＩＤ情報とから、ポートの状態を判断し、パケットのリピートに関するポートを制御するポート制御部１７とを備えているので、パケット内容を、ソースノードとデスティネイションノード間経路上のノード以外のノードに流さないようにすることが可能になり、パケット内容を盗聴される可能性を減ずることができる。
（第１４の実施の形態）
【０１８２】図１５は、本発明の第１４の実施の形態のリピート方法を示すフローチャートを示す。同図に示すように、ステップＳ１０１において、ネットワークのトポロジ情報を獲得する。ステップＳ１０４において、バスリセットの発生を待機する。ステップＳ１０４において、バスリセットが検出された場合、ステップＳ１０１へ戻り、検出されない場合はステップＳ１６１へ進む。ステップＳ１６１において、パケットの受信を待機する。ステップＳ１６１において、パケットが受信されない場合は、ステップＳ１０４へ戻り、パケットが受信された場合、ステップＳ１６２へ進む。ステップＳ１６２において、ポートのリピートを後述するように制御する。
【０１８３】図２に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップＳ１６２におけるポート制御の方法を説明する。同図に示すように、このネットワークは、ノード２０１～２１０とリピータ装置７１からなる。
【０１８４】パケットのデスティネイションＩＤが３であった場合、このパケットはＩＤ＝３のノード２０４が接続されているポートＰ２のみにリピートすれば、パケットの役割を果たすことができるため、それ以外のポート、ポートＰ０およびポートＰ１にはリピートする必要はない。
【０１８５】しかし、バスを占有していることを示すために、何らかのデータをドライブする必要はある。そこでポート制御部１７は以下のようにポートを制御する。
【０１８６】ポートＰ２は通常どおりにパケットのリピートを行う。パケットを受信したポートには通常どおりにリピートを行わない。ポートＰ０およびポートＰ１には、パケットと同サイズのダミーをリピートする。ダミーとしては、パケットのデータペイロード等重要と思われる部分を書き換えたもの、あらかじめ用意してある無害なパケット、が考えられ、またパケットでなくｄａｔａ　ｐｒｅｆｉｘを出しつづけても良い。
【０１８７】以上のように、本発明の第１４の実施の形態のリピート方法は、ネットワークのトポロジ情報を記憶し、パケットのデスティネイションＩＤを識別し、記憶されたトポロジ情報と、識別されたデスティネイションＩＤ情報とから、ポートの状態を判断し、パケットのリピートに関するポートを制御するので、パケット内容をソースノードとデスティネイションノード間経路上のノード以外のノードに流さないようにすることが可能になり、パケット内容を盗聴される可能性を減ずることができる。
（第１５の実施の形態）
【０１８８】本発明の第１５の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９から警告を受ける警告受信部（図示無し）と、警告発生時状態を収集する情報収集部（図示無し）と、この収集された情報をユーザに通知する表示部（図示無し）とを備えている。
【０１８９】ここで表示する内容は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告を出したノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容および、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在をユーザに示すことができる。
（第１６の実施の形態）
【０１９０】本発明の第１６の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップＳ１０５の各種処理で発生された警告を受けた場合に、警告内容と警告発生時の状態をユーザに通知するよう表示する。
【０１９１】ここで表示する内容は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告を出したノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容および、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在をユーザに示すことができる。
（第１７の実施の形態）

【０１９２】本発明の第１７の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９から警告を受ける警告受信部（図示無し）と、警告発生時状態を収集する情報収集部（図示無し）と、公衆回線に接続された公衆回線通信部（図示無し）とを備えている。

【０１９３】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９の何れかから警告を受けた場合に、警告内容を公衆回線に伝送する。

【０１９４】電話回線を利用して電話、携帯電話、ＰＨＳ、ページャ等に接続して異常を知らせても良い。また、必要な情報を音声メッセージに変換して、電話、携帯電話、ＰＨＳ等で情報を知らせても良い。さらに、コードに変換して携帯電話、ＰＨＳ、ページャ等に表示させる、画像にしてＦＡＸ信号にて伝送しても良い。

【０１９５】また、インターネットを利用して、電子メイル、常時接続型のアプリケーション、プッシュ配信型のアプリケーション、Ｗｅｂサーバ等を用いて必要な情報を伝達しても良い。これにより、不正な機器の存在を遠隔地のユーザに示すことができる。

（第１８の実施の形態）

【０１９６】本発明の第１８の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップＳ１０５の各種処理で発生された警告を受けた場合に、警告内容を公衆回線に伝送する。

【０１９７】電話回線を利用して電話、携帯電話、ＰＨＳ、ページャ等に接続して異常を知らせても良い。また、必要な情報を音声メッセージに変換して、電話、携帯電話、ＰＨＳ等で情報を知らせても良い。さらに、コードに変換して携帯電話、ＰＨＳ、ページャ等に表示させる、画像にしてＦＡＸ信号にて伝送しても良い。

【０１９８】また、インターネットを利用して、電子メイル、常時接続型のアプリケーション、プッシュ配信型のアプリケーション、Ｗｅｂサーバ等を用いて必要な情報を伝達しても良い。これにより、不正な機器の存在を遠隔地のユーザに示すことができる。

（第１９の実施の形態）

【０１９９】本発明の第１９の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９から警告を受ける警告受信部（図示無し）と、警告発生時状態を収集する情報収集部（図示無し）と、情報を記録する記憶部（図示無し）とを備えている。

【０２００】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９の何れかから警告を受けた場合に、警告の内容と警告発生時の状態等の情報を記録する。

【０２０１】ここで記録する情報は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告を出したノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在を記録し、後から参照できる。

（第２０の実施の形態）

【０２０２】本発明の第２０の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップＳ１０５の各種処理で発生された警告を受けた場合に、情報を記録する。

【０２０３】ここで記録する情報は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告を出したノードのＩＤ、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在を記録し、後から参照できる。

（第２１の実施の形態）

【０２０４】本発明の第２１の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９から警告を受ける警告受信部（図示無し）と、警告に関連する機器の挙動または状態を収集する情報収集部（図示無し）と、情報を記録する記憶部（図示無し）とを備えている。

【０２０５】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９の何れかから警告を受けた場合に、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録する。記録は、不正な機器をブラックリストとして登録し、さらにブラックリスト上の機器を監視する。

【０２０６】ここで監視内容としては、機器に関連するパケットを監視および記録しても良いし、機器のレジスタを一定間隔、またはバスリセット毎に取得および記録しても良い。また、ブラックリストの管理は、一定時間不正が発見されなかった場合リストから消去しても良いし、機器認証を行い正常であることが確認された後リストから消去しても良い。あるいは、ネットワークから削除されたのを確認したらリストから消去しても良い。リストから消去する替わりに、休眠状態にする、監視のレベルを変化させても良い。これにより、不正な機器の存在およびその挙動を記録し、後から参照でき、不正な挙動を発見できる。

（第２２の実施の形態）

【０２０７】本発明の第２２の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップＳ１０５の各種処理で発生された警告を受けた場合に、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録する。記録は、不正な機器をブラックリストとして登録し、さらにブラックリスト上の機器を監視する。

【０２０８】ここで監視内容としては、機器に関連するパケットを監視および記録しても良いし、機器のレジスタを一定間隔、またはバスリセット毎に取得および記録しても良い。また、ブラックリストの管理は、一定時間不正が発見されなかった場合リストから消去しても良いし、機器認証を行い正常であることが確認された後リストから消去しても良い。あるいは、ネットワークから削除されたのを確認したらリストから消去しても良い。リストから消去する替わりに、休眠状態にする、監視のレベルを変化させても良い。これにより、不正な機器の存在およびその挙動を記録し、後から参照でき、不正な挙動を発見できる。

（第２３の実施の形態）

【０２０９】本発明の第２３の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９から警告を受ける警告受信部（図示無し）と、他機器にサービスを提供するサービス処理部と、条件によりサービスの提供の許可を行うサービス制御部とを備えている。

【０２１０】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９の何れかから警告を受けた場合に、サービスを停止する。ここでサービスの停止とは、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することである。

【０２１１】サービス停止としては、不正な機器との間に張られているコネクションを切断しても良いし、不正な機器からのアクセスを許可しないようにしても良いし、不正な機器からのパケットを受信しないようにしても良い。あるいは、サービス停止の替わりにサービスを変更しても良い。サービス変更とは、アクセスレベルを制限する、サービス内容を制限する、または不正な機器専用のサービスを用意しておき供給する等が考えられる。これにより、不正な機器に供与するサービスに制限を与え、不正な機器による被害を制限できる。

（第２４の実施の形態）

【０２１２】本発明の第２４の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップＳ１０５の各種処理で発生された警告を受けた場合に、サービスを停止する。

【０２１３】ここでサービスの停止とは、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することである。

【０２１４】サービス停止としては、不正な機器との間に張られているコネクションを切断しても良いし、不正な機器からのアクセスを許可しないようにしても良いし、不正な機器からのパケットを受信しないようにしても良い。あるいは、サービス停止の替わりにサービスを変更しても良い。サービス変更とは、アクセスレベルを制限する、サービス内容を制限する、または不正な機器専用のサービスを用意しておき供給する等が考えられる。これにより、不正な機器に供与するサービスに制限を与え、不正な機器による被害を制限できる。

（第２５の実施の形態）

【０２１５】本発明の第２５の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９から警告を受ける警告受信部（図示無し）と、パケットのルーティングを行うルーティング部（図示無し）と、ルーティングの設定を行うルーティング制御部（図示無し）とを備えている。

【０２１６】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置１、２１、３１、４１、５１および６１の各種処理部９の何れかから警告を受けた場合に、警告に関連した機器の何れかまたは全てからのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更する。

【０２１７】例として、不正な機器に関連するルーティングを停止する。あるいは停止する代わりに、通常は不正な機器にルーティングされるべきパケットを、不正機器を監視している機器にルーティングするようにしても良い。また、不正な機器から送出されたパケットを、同様に不正機器を監視している機器にルーティングするようにしても良い。あるいは上記パケットを通常のルーティング経路とは異なる、不正ノード用の経路にルーティングをするようにしても良いし、特定のエリアには不正ノード関連のパケットを侵入させないようにしても良い。

【０２１８】これにより、不正な機器からのパケットのルーティングをコントロールでき、記録が容易に行える、あるいは不正な機器による被害を制限できる。

（第２６の実施の形態）

【０２１９】本発明の第２６の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップＳ１０５の各種処理で発生された警告を受けた場合に、警告に関連した機器の何れかまたは全てからのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更する。

【0220】例として、不正な機器に関連するルーティングを停止する。あるいは停止する代わりに、通常は不正な機器にルーティングされるべきパケットを、不正機器を監視している機器にルーティングするようにしても良い。また、不正な機器から送出されたパケットを、同様に不正機器を監視している機器にルーティングするようにしても良い。あるいは上記パケットを通常のルーティング経路とは異なる、不正ノード用の経路にルーティングをするようにしても良いし、特定のエリアには不正ノード関連のパケットを侵入させないようにしても良い。

【0221】これにより、不正な機器からのパケットのルーティングをコントロールでき、記録が容易に行える、あるいは不正な機器による被害を制限できる。

（第27の実施の形態）

【0222】本発明の第27の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部（図示無し）と、機器の認証機能を備えた機器認証部とを備えている。

【0223】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、関連する機器に対し機器認証を行う、またはやり直す。

【0224】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0225】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

（第28の実施の形態）

【0226】本発明の第28の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、機器認証を行う、または機器認証をやり直す。

【0227】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0228】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

（第29の実施の形態）

【0229】本発明の第29の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部（図示無し）と、データの暗号化を行う暗号部とを備えている。

【0230】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、データの暗号化を行う、または暗号化キーを再作成する。

【0231】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

（第30の実施の形態）

【0232】本発明の第30の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、通信を暗号化する、または暗号化キーを作成し直すようにする。

【0233】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

【0234】

【発明の効果】以上説明したように、本発明はネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視方法を提供することができるものである。

【0235】また、本発明はネットワークのトポロジ情報を記憶するトポロジ記憶部と、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視装置を提供することができるものである。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図2】実施の形態の挙動を説明するためのネットワーク構成例を示すブロック図

【図3】本発明の第2の実施の形態のネットワーク監視方法を示すフローチャート

【図4】本発明の第3の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図5】本発明の第4の実施の形態のネットワーク監視方法を示すフローチャート

【図6】本発明の第5の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図7】本発明の第6の実施の形態のネットワーク監視方法を示すフローチャート

【図8】本発明の第7の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【0220】例として、不正な機器に関連するルーティングを停止する。あるいは停止する代わりに、通常は不正な機器にルーティングされるべきパケットを、不正機器を監視している機器にルーティングするようにしても良い。また、不正な機器から送出されたパケットを、同様に不正機器を監視している機器にルーティングするようにしても良い。あるいは上記パケットを通常のルーティング経路とは異なる、不正ノード用の経路にルーティングをするようにしても良いし、特定のエリアには不正ノード関連のパケットを侵入させないようにしても良い。

【0221】これにより、不正な機器からのパケットのルーティングをコントロールでき、記録が容易に行える、あるいは不正な機器による被害を制限できる。

(第27の実施の形態)

【0222】本発明の第27の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、機器の認証機能を備えた機器認証部とを備えている。

【0223】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、関連する機器に対し機器認証を行う、またはやり直す。

【0224】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0225】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

(第28の実施の形態)

【0226】本発明の第28の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、機器認証を行う、または機器認証をやり直す。

【0227】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0228】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

(第29の実施の形態)

【0229】本発明の第29の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、データの暗号化を行う暗号部とを備えている。

【0230】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、データの暗号化を行う、または暗号化キーを再作成する。

【0231】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

(第30の実施の形態)

【0232】本発明の第30の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、通信を暗号化する、または暗号化キーを作成し直すようにする。

【0233】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

【0234】

【発明の効果】以上説明したように、本発明はネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視方法を提供することができるものである。

【0235】また、本発明はネットワークのトポロジ情報を記憶するトポロジ記憶部と、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視装置を提供することができるものである。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図2】実施の形態の挙動を説明するためのネットワーク構成例を示すブロック図

【図3】本発明の第2の実施の形態のネットワーク監視方法を示すフローチャート

【図4】本発明の第3の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図5】本発明の第4の実施の形態のネットワーク監視方法を示すフローチャート

【図6】本発明の第5の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

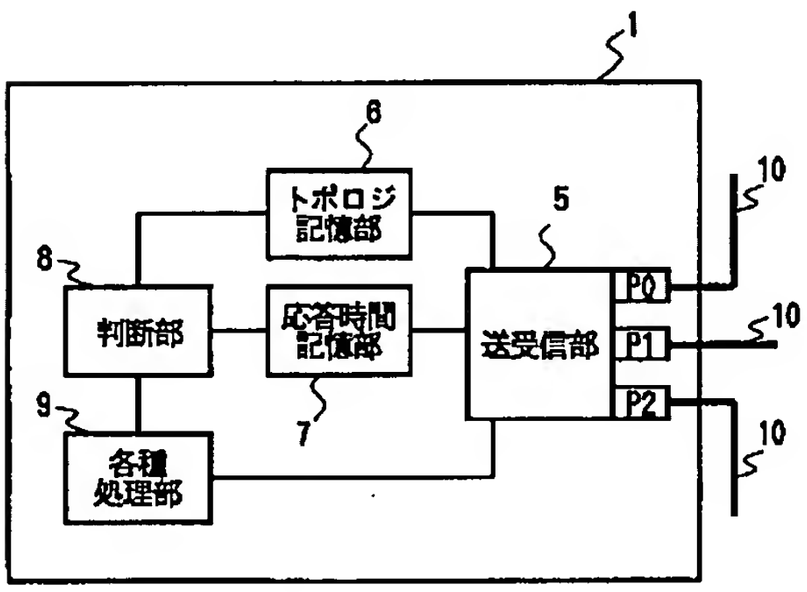
【図7】本発明の第6の実施の形態のネットワーク監視方法を示すフローチャート

【図8】本発明の第7の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

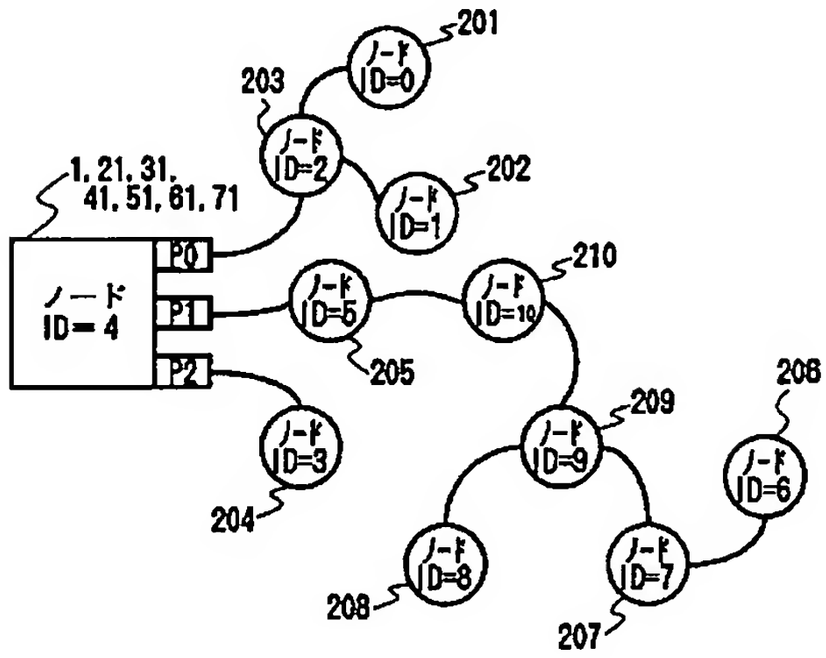
【図９】本発明の第８の実施の形態のネットワーク監視方法を示すフローチャート
【図１０】本発明の第９の実施の形態のネットワーク監視装置の構成を示す概略ブロック図
【図１１】本発明の第１０の実施の形態のネットワーク監視方法を示すフローチャート
【図１２】本発明の第１１の実施の形態のネットワーク監視装置の構成を示す概略ブロック図
【図１３】本発明の第１２の実施の形態のネットワーク監視方法を示すフローチャート
【図１４】本発明の第１３の実施の形態のリピータ装置の構成を示す概略ブロック図
【図１５】本発明の第１４の実施の形態のリピート方法を示すフローチャート

【符号の説明】
1、21、31、41、51、61　ネットワーク監視装置
5　送受信部
6　トポロジ記憶部
7　応答時間記憶部
8　判断部
9　各種処理部
10　バス
P0、P1、P2　ポート
11　ソース識別部
12　時間測定部
13　ソース順番識別部
14　ACKソース順番識別部
15　ルーティングテーブル確認部
16　デスティネイション識別部
17　ポート制御部
71　リピータ装置

【図１】

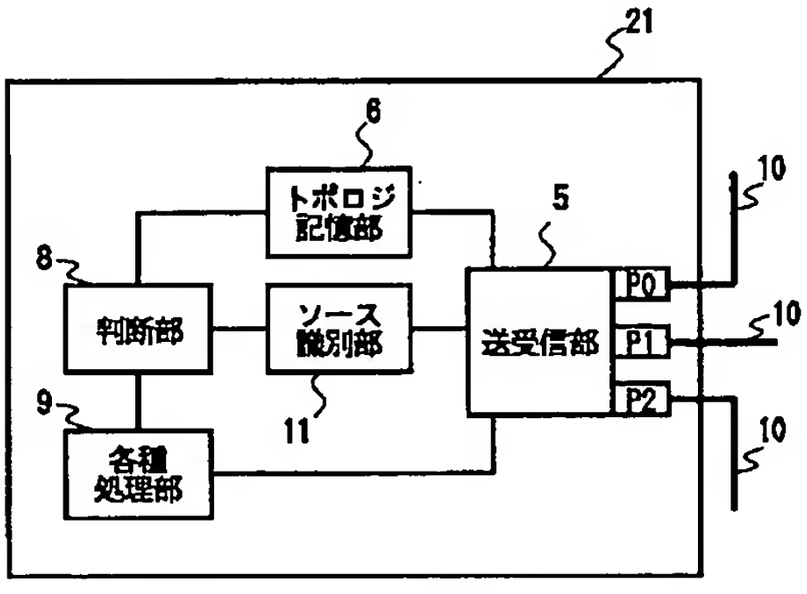


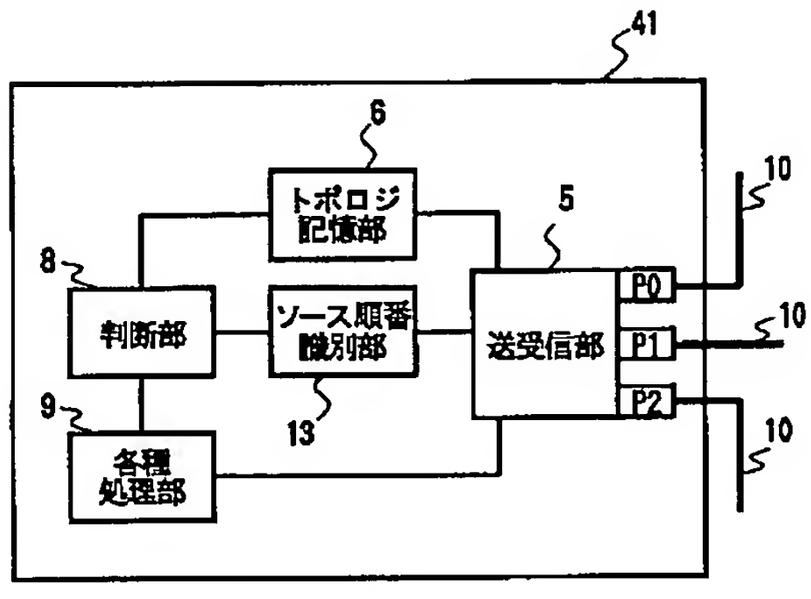
【図２】



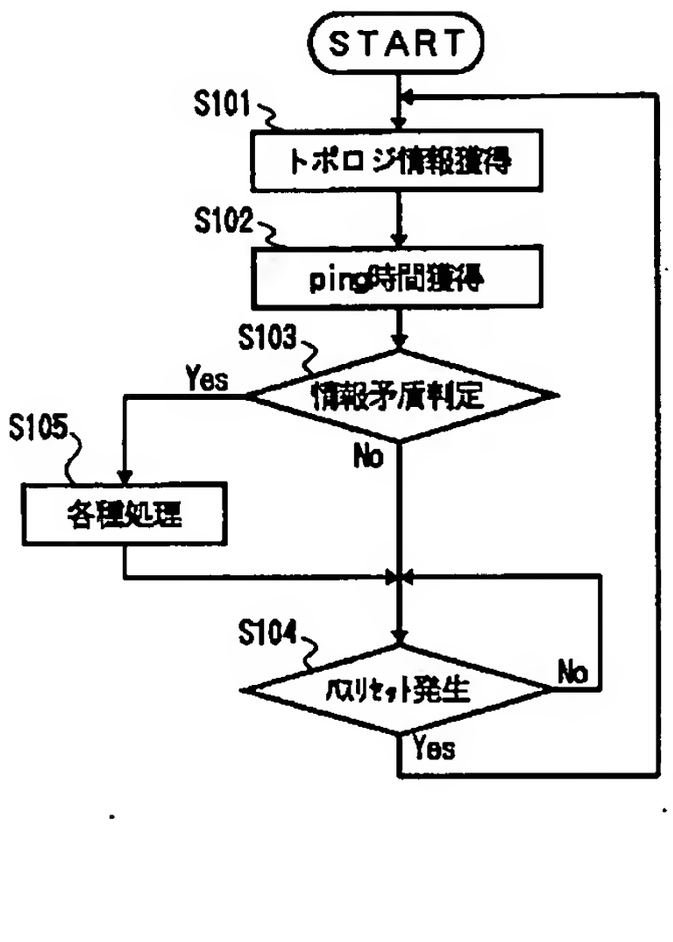
【図８】

【図４】

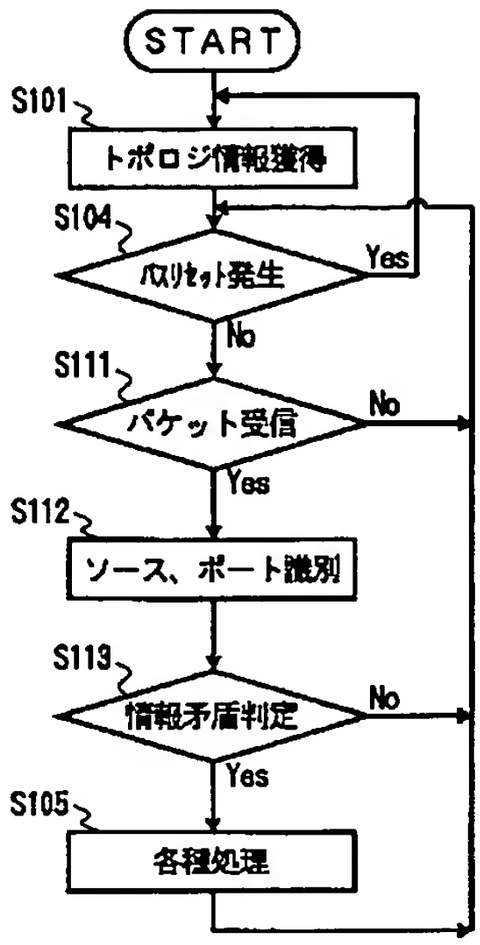




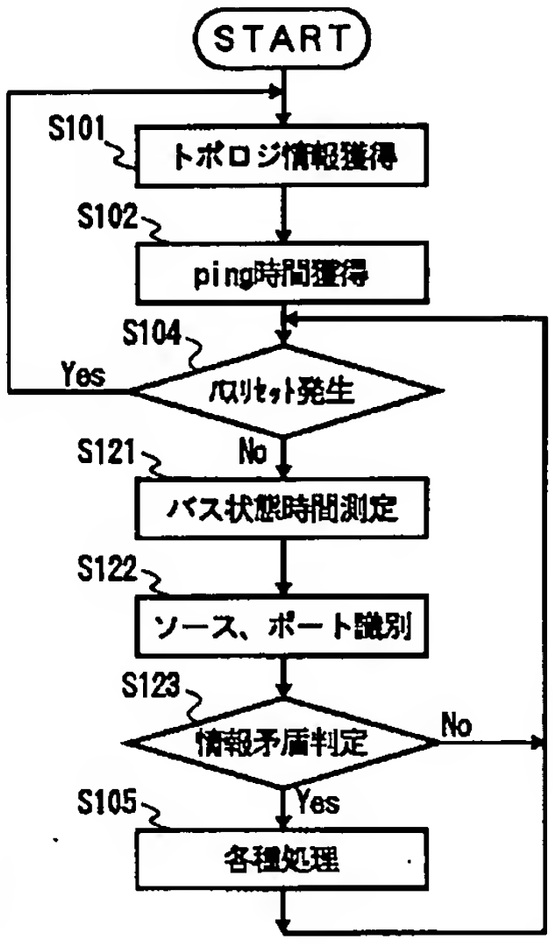
【図3】



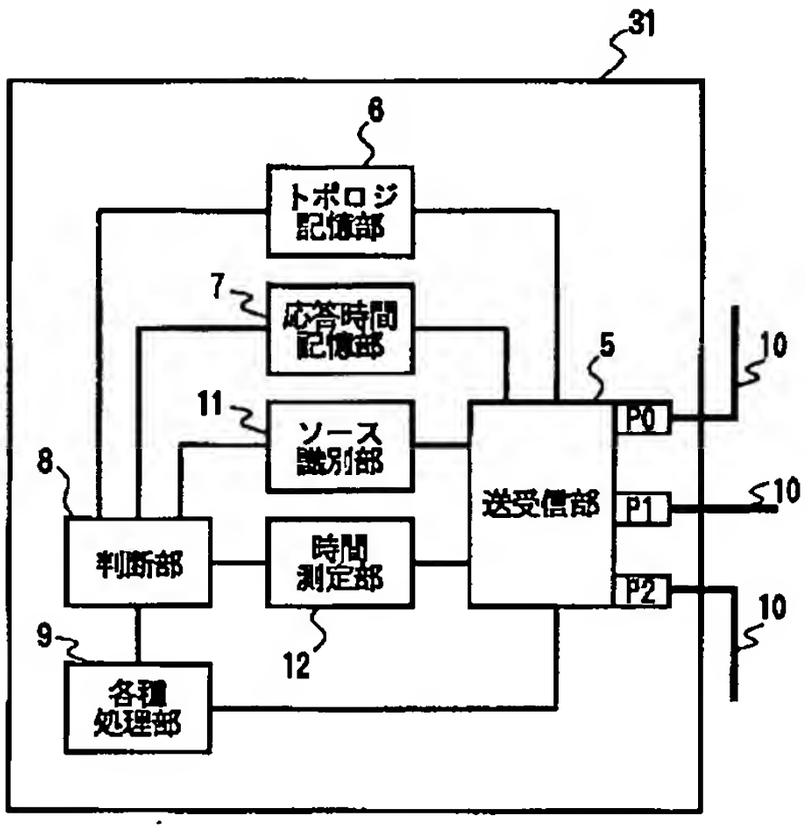
【図5】



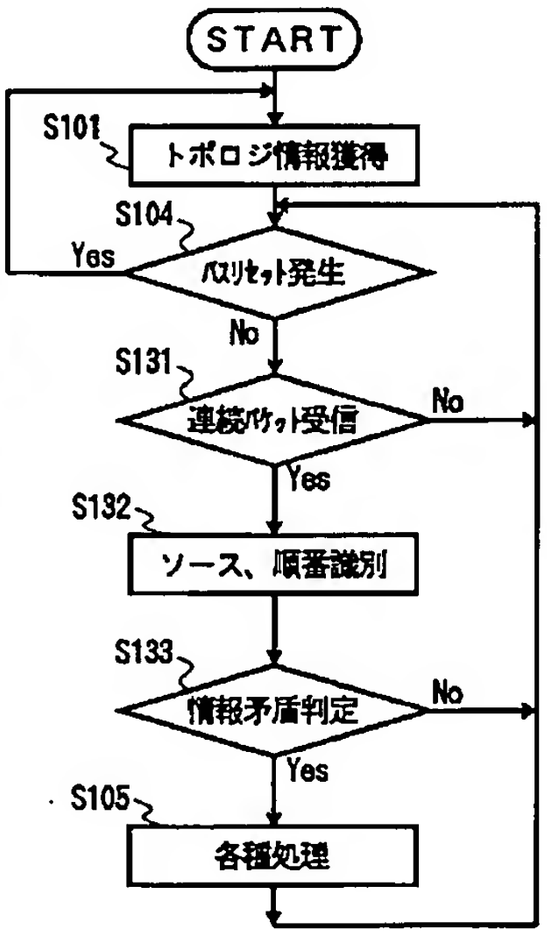
【図7】



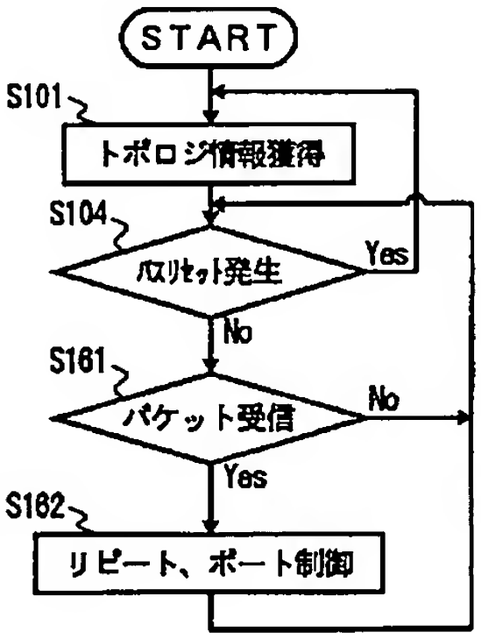
【図6】



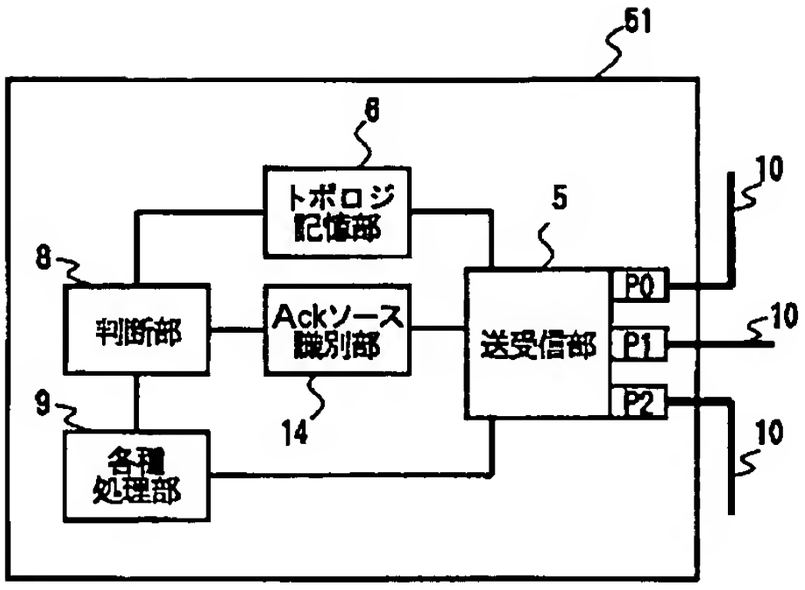
【図9】



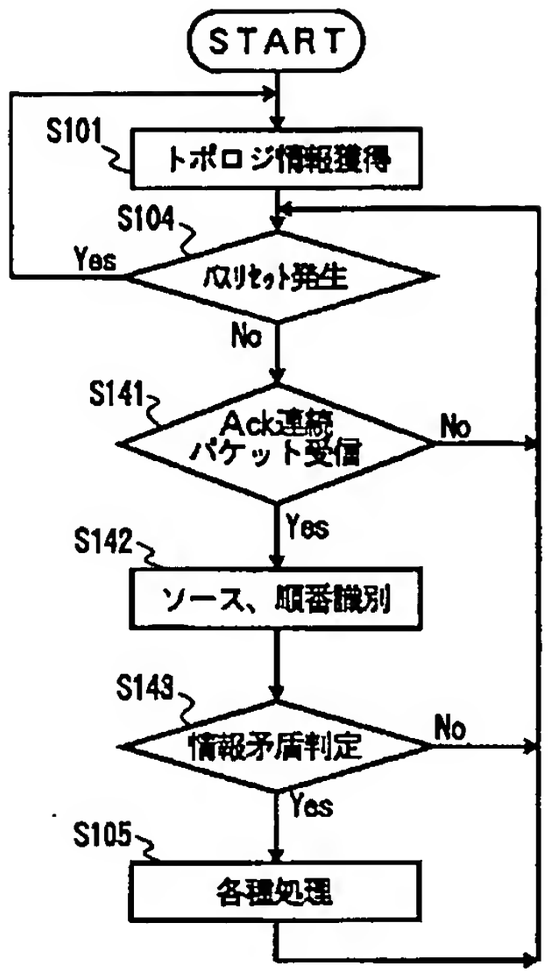
【図15】



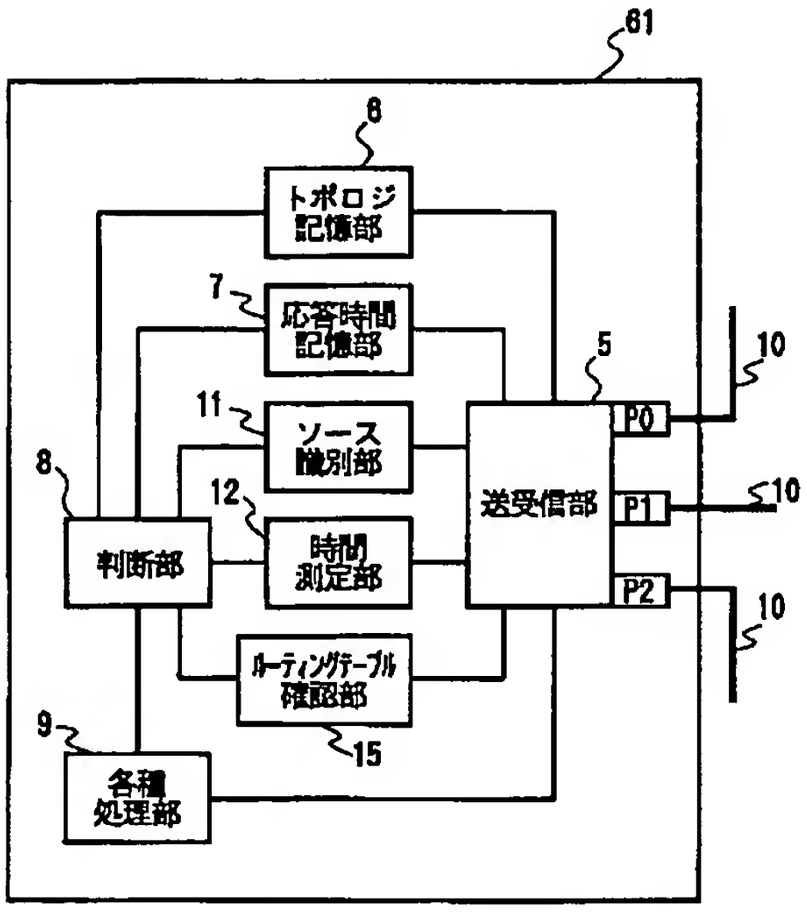
【図10】



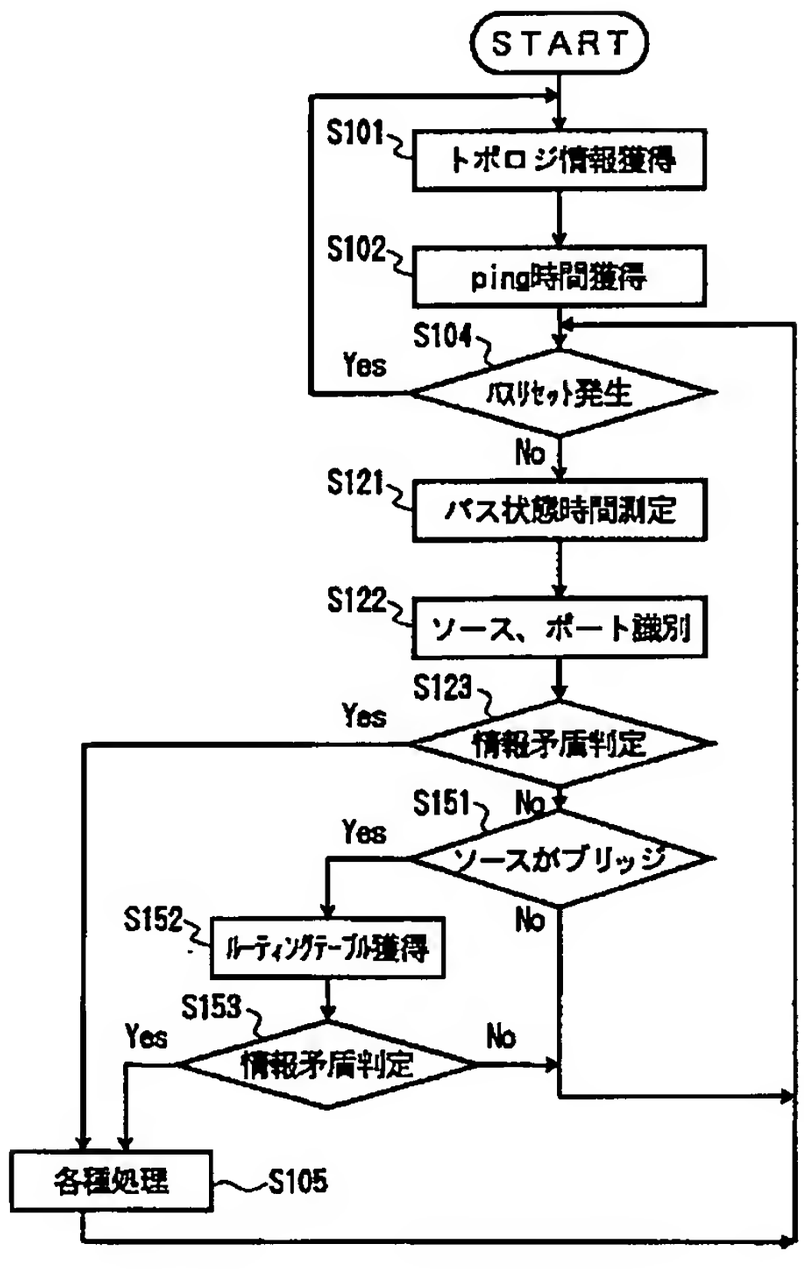
【図11】



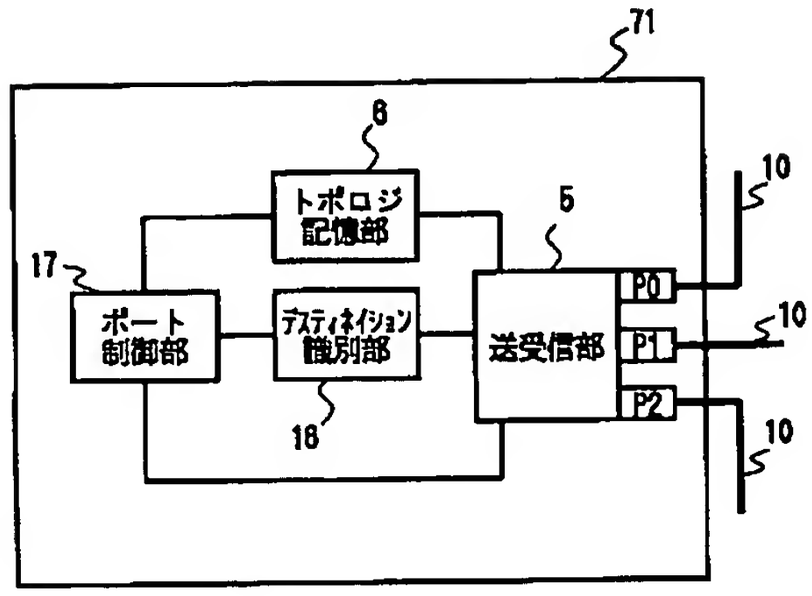
【図12】



【図13】



【図14】



フロントページの続き

Fターム(参考) 5K030 GA15 HA08 HB06 HB28 HB29
KA07 LA02 MA06 MC04 MC06
MC09
5K033 AA08 CB04 CC01 DA13 DB20
EA05
5K035 EE03 EE05 GG01 MM02 MM06